HP ProtectTools

お使いになる前に

目次

1 はじめに

HP ProtectTools セキュリティ マネージャ ソフトウェアは、コンピュータ本体、ネットワーク、および重要なデータを不正なアクセスから保護するために役立つセキュリティ機能を提供します。以下のソフトウェア モジュールによって、高度なセキュリティ機能が提供されます。

- スマート カード セキュリティ
- Java Card Security for HP ProtectTools
- Embedded Security for HP ProtectTools
- BIOS Configuration for HP ProtectTools
- Credential Manager for HP ProtectTools
- Device Access Manager for HP ProtectTools

コンピュータで利用可能なソフトウェア モジュールは、モデルによって異なる可能性があります。たとえば、Embedded Security for HP ProtectTools を使用するには、TPM（Trusted Platform Module）内蔵セキュリティ チップ（一部のモデルのみ）がコンピュータに搭載されている必要があり、また、スマート カード セキュリティを使用するにはオプションのスマート カードおよびリーダーが必要です。

HP ProtectTools ソフトウェア モジュールは、プリインストールまたはプリロードされている場合と、HP の Web サイトからダウンロードできる場合があります。詳しくは、http://www.hp.com/jp/にアクセスしてください。

注記　このガイドの指示は、該当する HP ProtectTools ソフトウェア モジュールがすでにインストールされていることを前提に書かれています。

HP ProtectTools セキュリティ マネージャへのアクセス

Windows®の[コントロール パネル]から HP ProtectTools セキュリティ マネージャにアクセスするには、次の操作を行います。

▲ **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。

注記　Credential Manager モジュールを設定した後は、Windows のログオン画面から直接 Credential Manager にログオンして HP ProtectTools を起動することもできます。詳しくは、「第 6 章 Credential Manager for HP ProtectTools」の「Credential Manager を使用した Windows へのログオン」を参照してください。

セキュリティの役割について

コンピュータのセキュリティを（特に、大きな組織で）管理する上では、責任および権限をさまざまな管理者やユーザに割り当てることが、重要な作業の 1 つです。

注記　小さな組織や個人で使用する場合は、一人の人がすべての役割を持っていても構いません。

HP ProtectTools では、セキュリティの責任および権限を以下の役割に分割できます。

- セキュリティ オフィサ：企業またはネットワークのセキュリティ レベルを定義し、スマート カード、指紋認証システム、USB トークンなど、配備するセキュリティ機能を決定します。

注記　HP ProtectTools の機能の多くは、セキュリティ オフィサが HP と協力してカスタマイズできます。詳しくは、http://www.hp.com/jp/にアクセスしてください。

- IT 管理者：セキュリティ オフィサによって定義されたセキュリティ機能を適用し、管理します。また、一部の機能を有効または無効にできます。たとえば、セキュリティ オフィサがスマート カードの配備を決定した場合、IT 管理者はスマート カードの BIOS セキュリティ モードを有効にすることができます。
- ユーザ：セキュリティ機能を使用します。たとえば、セキュリティ オフィサおよび IT 管理者がシステムでスマート カードを有効にしている場合、ユーザはスマート カードの PIN を設定し、そのカードを認証に使用できます。

HP ProtectTools のパスワードの管理

HP ProtectTools セキュリティ マネージャの機能のほとんどは、パスワードによってセキュリティ保護されています。次の表に、よく使用されるパスワード、そのパスワードが設定されるソフトウェア モジュール、およびパスワード機能の一覧を示します。

この表には、IT 管理者だけが設定して使用するパスワードも示されています。その他のすべてのパスワードは、一般のユーザまたは管理者が設定できます。

HP ProtectTools のパスワード	設定する HP ProtectTools モジュール	機能
[Computer Setup]のセットアップ パスワード **注記** BIOS の管理者パスワード、f10 セットアップ パスワード、またはセキュリティ セットアップ パスワードとも呼ばれます	BIOS Configuration、IT 管理者が設定	[Computer Setup]ユーティリティへのアクセスを保護します
Power-on Password（電源投入時パスワード）	BIOS Configuration	コンピュータの起動時や再起動時、またはハイバネーションからの復帰時にコンピュータのデータを保護します
スマート カードの管理者パスワード **注記** BIOS 管理者カードのパスワードとも呼ばれます	スマート カード セキュリティ、IT 管理者が設定	スマート カードの電源投入時（BIOS）認証に使用します。コンピュータの起動時や再起動時、またはハイバネーションからの復帰時に[Computer Setup]ユーティリティおよびコンピュータのデータへのアクセスを可能にします。また、ユーザ カードまたは管理者カードの復元のためのリカバリ ファイルの作成も可能になります
スマート カードのユーザ パスワード **注記** BIOS ユーザ カードのパスワードとも呼ばれます	スマート カード セキュリティ	スマート カードの電源投入時（BIOS）認証に使用します。コンピュータの起動時や再起動時、またはハイバネーションからの復帰時にコンピュータのデータへのアクセスを可能にします
スマート カードの PIN	スマート カード セキュリティ	スマート カードの内容へのアクセスを保護し、スマート カードのユーザを認証します。電源投入時認証に使用すると、スマート カードの PIN の入力により[Computer Setup]ユーティリティおよびコンピュータのデータも保護されます
スマート カード リカバリ ファイルのパスワード	スマート カード セキュリティ	BIOS パスワードが含まれているリカバリ ファイルへのアクセスを保護します
Java™ Card の PIN	Java Card Security	Java Card の内容へのアクセスを保護し、Java Card のユーザを認証します。電源投入時認証に使用すると、Java Card の PIN の入力により[Computer Setup]ユーティリティおよびコンピュータのデータも保護されます
基本ユーザ キーのパスワード	Embedded Security	安全な電子メール、ファイル、およびフォルダの暗号化など Embedded Security 機能へのアクセスに使用します。電源投入時認

HP ProtectTools のパスワード	設定する HP ProtectTools モジュール	機能
注記 内蔵セキュリティ パスワードとも呼ばれます		証に使用すると、コンピュータの起動時や再起動時、またはハイバネーションからの復帰時にコンピュータのデータを保護します
緊急リカバリ トークンのパスワード **注記** 緊急リカバリ トークン キーのパスワードとも呼ばれます	Embedded Security、IT 管理者が設定	内蔵セキュリティ チップ用のバックアップ ファイルである緊急リカバリ トークンへのアクセスを保護します
所有者のパスワード	Embedded Security、IT 管理者が設定	システムと TPM チップを、Embedded Security のすべての所有者機能への不正なアクセスから保護します
Credential Manager のログオン パスワード	Credential Manager	このパスワードには、次の 2 つのオプションがあります ● Windows にログオンした後、Credential Manager にアクセスするための別のログオンで使用できます ● Windows ログオン プロセスの代わりに使用し、Windows と Credential Manager に同時にアクセスできます
Credential Manager リカバリ ファイルのパスワード	Credential Manager、IT 管理者が設定	Credential Manager リカバリ ファイルへのアクセスを保護します
Windows のログオン パスワード	Windows の[コントロール パネル]	手動ログオンで使用するか、またはスマート カードに保存できます

セキュリティ保護されたパスワードの作成

パスワードを作成する場合は、まず、プログラムで設定されている仕様に従う必要があります。ただし一般的には、強力なパスワードを作成して、作成したパスワードが危険にさらされないようにするために、以下のガイドラインを考慮してください。

- 文字数が 6 文字、できれば 8 文字を超えるパスワードを使用します。
- パスワード全体にわたって大文字と小文字を混在させせます。
- 可能な場合は常に、半角英数字を混在させ、さらに特殊文字と句読点を含めます。
- パスワード中の文字の代わりに特殊文字または数字を使用します。たとえば、アルファベットの l または L の代わりに数字の 1 を使用します。
- 2 つ以上の言語から取った単語を組み合わせます。
- 単語またはフレーズを数字や特殊文字で分割します。たとえば、「Mary2-2Cat45」とします。
- 辞書に載っているような用語は使用しないでください。
- 名前やその他の個人情報（たとえば、誕生日、ペットの名前、母親の旧姓など）は、たとえ綴りを逆にしたとしても、パスワードには使用しないでください。
- パスワードは定期的に変更してください。いくつかの文字や数字を次の値に変更するだけでも構いません。
- パスワードをメモした場合は、コンピュータのすぐ近くの、人目につきやすい場所に保管しないでください。
- パスワードを、電子メールなどのコンピュータ上のファイルに保存しないでください。
- アカウントを共有したり、パスワードを誰かに教えたりしないでください。

2　スマート カード セキュリティ

スマート カード セキュリティは、オプションのスマート カード リーダーが装備されたコンピュータでのスマート カードのセットアップおよび設定を管理します。

スマート カード セキュリティを使用すると、次のことができます。

- スマート カードのセキュリティ機能にアクセスできます。
- Credential Manager for HP ProtectTools などの他の HP ProtectTools モジュールで使用できるようにスマート カードを初期化できます。
- [Computer Setup]ユーティリティを使用して電源投入時の環境でスマート カードの認証を可能にし、またスマート カードを管理者用とユーザ用に分けて設定できます。これにより、オペレーティング システムをロードさせるには、ユーザがスマート カードを挿入し PIN を入力することが必要となります（PIN の入力はオプションです）。
- スマート カードのユーザ認証を行うためのパスワードの設定および変更を行えます。
- スマート カードに格納されているスマート カードの BIOS パスワードのバックアップおよびリストア（復元）を行えます。

スマート カードの初期化

スマート カードは、使用する前に初期化する必要があります。

スマート カードを初期化するには、以下の手順で操作します。

1. スマート カードをリーダーに挿入します。
2. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
3. 左側のパネルで、**[Smart Card Security]**（スマート カード セキュリティ）をクリックし、**[Smart Card]**（スマート カード）をクリックします。
4. 右側のパネルで、**[Initialize]**（初期化）をクリックします。
5. **[Initialize the smart card]**（スマート カードの初期化）ダイアログ ボックスの最初のボックスに名前を入力します。
6. 適切なボックスにスマート カードの PIN を設定して確定します。PIN は、4 ～ 8 桁の半角数字にする必要があります。

注意 コンピュータにアクセスできなくなることを防ぐため、スマート カードの PIN を忘れないようにしてください。スマート カードの PIN を忘れると、コンピュータの操作が不可能になることがあります。スマート カードはロックされ、スマート カードの PIN を 5 回以内の試行で正しく入力しないと使用できなくなります。この試行のカウントは、正しい PIN が入力されるとリセットされます。

7. **[OK]**をクリックして初期化を完了します。

スマート カードの BIOS セキュリティ モード

スマート カードの BIOS セキュリティ モードが有効になると、スマート カードを使用してコンピュータを起動することが必要になります。

スマート カードの BIOS セキュリティ モードを有効にするプロセスには、以下の手順が含まれます。

1. BIOS Configuration で、スマート カードの電源投入時認証サポートを有効にします。「第 5 章 BIOS Configuration for HP ProtectTools」の「スマート カードまたは Java Card の電源投入時認証サポートの有効/無効の設定」を参照してください。

注記 この設定を有効にすると、電源投入時認証にスマート カードを使用できるようになります。スマート カードの電源投入時認証サポートを有効にするまで、スマート カードの BIOS セキュリティ モード機能は使用できません。

2. スマート カード セキュリティで、スマート カードの BIOS セキュリティ モードを有効にします。この章の「スマート カードの BIOS セキュリティ モードの有効化とスマート カードの管理者パスワードの設定」を参照してください。

3. スマート カードの管理者パスワードを設定します。

注記 スマート カードの管理者パスワードは、スマート カードの BIOS セキュリティ モードを有効にするプロセスの一部として設定されます。

スマート カードの管理者パスワードは、[Computer Setup]のセットアップ パスワードとは異なります。スマート カードの管理者パスワードにより、識別のためにスマート カードがコンピュータにリンクされるだけでなく、以下のことも可能になります。

- コンピュータの電源投入後の、[Computer Setup]またはコンピュータのデータへのアクセス
- 新しい管理者およびユーザのスマート カードの作成
- ユーザ用または管理者用のどちらかのスマート カードを復元するためのリカバリ ファイルの作成

スマート カードの BIOS セキュリティ モードの有効化とスマート カードの管理者パスワードの設定

スマート カードの BIOS セキュリティ モードを有効にしてスマート カードの管理者パスワードを設定するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Smart Card Security]**（スマート カード セキュリティ）をクリックし、**[BIOS]**をクリックします。
3. 右側のパネルで、[BIOS Security Mode]（BIOS セキュリティ モード）の**[Enable]**（有効にする）をクリックします。
4. **[Next]**（次へ）をクリックします。
5. プロンプトで[Computer Setup]のセットアップ パスワードを入力して**[Next]**をクリックします。
6. 新しい管理者スマート カードを挿入し、画面の説明に沿って操作します。手順が異なっても、以下のタスクは含まれている可能性があります。
   - スマート カードの初期化。詳しい手順については、「スマート カードの初期化」を参照してください。
   - スマート カードの管理者パスワードの設定。詳しい手順については、「管理者カードまたはユーザ カードのパスワードの格納」を参照してください。
   - リカバリ ファイルの作成。詳しい手順については、「リカバリ ファイルの作成」を参照してください。

スマート カードの BIOS セキュリティ モードの無効化

スマート カードの BIOS セキュリティ モードを無効にすると、スマート カードの管理者パスワードおよびユーザ パスワードは無効になり、コンピュータにアクセスするためにスマート カードを使用する必要はなくなります。

注記　以前にスマート カードの BIOS セキュリティ モードを有効にしている場合は、[Smart Card Security BIOS]（スマート カード セキュリティの BIOS）ページのボタンが[Disable]（無効にする）に変更されています。

スマート カード セキュリティを無効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Smart Card Security]**（スマート カード セキュリティ）をクリックし、**[BIOS]**をクリックします。
3. 右側のパネルで、**[BIOS Security Mode]**（BIOS セキュリティ モード）の**[Disable]**をクリックします。
4. 現在のスマート カードの管理者パスワードが含まれているカードを挿入して**[Next]**（次へ）をクリックします。
5. プロンプトでスマート カードの PIN を入力して**[Finish]**（完了）をクリックします。

スマート カードの管理者パスワードの変更

スマート カードの管理者パスワードは、スマート カードの BIOS セキュリティ モードを有効にするプロセスの一部として設定されます。スマート カードの管理者パスワードは、設定された後でも変更できます。スマート カードの管理者パスワードについて詳しくは、この章の「スマート カードの BIOS セキュリティ モード」を参照してください。

注記　以下の手順によって、カードと[Computer Setup]に格納されているスマート カードの管理者パスワードが更新されます。

カードの管理者パスワードを変更するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Smart Card Security]**（スマート カード セキュリティ）をクリックし、**[BIOS]**をクリックします。
3. 右側のパネルで、**[BIOS Security Mode]**（BIOS セキュリティ モード）の**[BIOS administrator card]**（BIOS 管理者カード）の横にある**[Change]**（変更）をクリックします。
4. スマート カードの PIN を入力して**[Next]**（次へ）をクリックします。
5. 新しい管理者カードを挿入して**[Next]**をクリックします。
6. スマート カードの PIN を入力して**[Finish]**（完了）をクリックします。

スマート カードのユーザ パスワードの設定と変更

スマート カードのユーザ パスワードを設定または変更するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Smart Card Security]**（スマート カード セキュリティ）をクリックし、**[BIOS]**をクリックします。
3. 右側のパネルで、**[BIOS Security Mode]**（BIOS セキュリティ モード）の**[BIOS user card]**（BIOS ユーザ カード）の横にある**[Set]**（設定）ボタンをクリックします。

   注記　[Computer Setup]にすでにユーザ パスワードが存在する場合は、**[Change]**（変更）ボタンをクリックします。

4. スマート カードの PIN を入力して**[Next]**（次へ）をクリックします。
5. 新しいユーザ カードを挿入して**[Next]**をクリックします。
   - カード上にユーザ パスワードが存在する場合は、**[Finish]**（完了）ダイアログ ボックスが表示されます。手順 6 ～ 8 を省略して手順 9 に進みます。
   - カード上にユーザ パスワードが存在しない場合は、[BIOS Password Wizard]（BIOS パスワード ウィザード）が起動します。
6. [BIOS Password Wizard]（BIOS パスワード ウィザード）で、次のどちらかを行うことができます。
   - パスワードを手動で入力します。
   - 32 バイトのランダムなパスワードを生成します。

   注記　既知のパスワードを使用すると、リカバリ ファイルを使用しないで複製カードを作成できます。ランダムなパスワードを生成するとセキュリティは強化されますが、バックアップ カードを作成するためにリカバリ ファイルが必要になります。

7. 起動時にスマート カードの PIN の入力を必要とする場合は、**[Boot Requirements]**（ブート要件）で該当のチェック ボックスにチェックを入れます。

   注記　起動時にスマート カードの PIN の入力を必要としない場合は、このチェック ボックスのチェックを外します。

8. スマート カードの PIN を入力して**[OK]**をクリックします。システムから、リカバリ ファイルを作成するよう要求されます。

   注記　リカバリ ファイルを作成することを強くおすすめします。詳しくは、この章の「リカバリ ファイルの作成」を参照してください。

9. **[Finish]**（完了）ダイアログ ボックスでスマート カードの PIN を入力して**[Finish]**をクリックします。

管理者カードまたはユーザ カードのパスワードの格納

バックアップ カードを作成するとき、管理者パスワードがすでに設定されている場合は、そのパスワードを新しいカードに格納できます。

注意 この手順ではカード上のパスワードだけが更新され、[Computer Setup]のパスワードは更新されません。新しいカードでコンピュータにアクセスすることはできません。

管理者カードまたはユーザ カードのパスワードを格納するには、以下の手順で操作します。

1. スマート カードをリーダーに挿入します。
2. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
3. 左側のパネルで、**[Smart Card Security]**（スマート カード セキュリティ）をクリックし、**[BIOS]**をクリックします。
4. 右側のパネルで、**[BIOS Password on Smart Card]**（スマート カードの BIOS パスワード）の**[Store]**（格納）をクリックします。
5. [BIOS Password Wizard]（BIOS パスワード ウィザード）で、次のどちらかを行うことができます。
   - パスワードを手動で入力します。
   - 32 バイトのランダムなパスワードを生成します。

   注記 既知のパスワードを使用すると、リカバリ ファイルを使用しないで複製カードを作成できます。ランダムなパスワードを生成するとセキュリティは強化されますが、バックアップ カードを作成するためにリカバリ ファイルが必要になります。

6. **[Access Privilege]**（アクセス権）で、カードの種類として**[Administrator]**（管理者）または**[User]**（ユーザ）のどちらかをクリックします。
7. **[Boot Requirements]**（ブート要件）で、起動時にスマート カードの PIN の入力を必要とする場合は該当のチェック ボックスにチェックを入れます。

   注記 起動時にスマート カードの PIN の入力を必要としない場合は、このチェック ボックスのチェックを外します。

8. スマート カードの PIN を入力して**[OK]**をクリックします。
9. **[Finish]**（完了）ダイアログ ボックスでスマート カードの PIN を再度入力して、**[Finish]**をクリックします。

   システムから、リカバリ ファイルを作成するよう要求されます。

   注記 スマート カード リカバリ ファイルを作成することを強くおすすめします。詳しくは、この章の「リカバリ ファイルの作成」を参照してください。

一般的なタスク

BIOS スマート カード設定の更新

コンピュータの再起動時にスマート カードの PIN を要求するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Smart Card Security]**（スマート カード セキュリティ）をクリックし、**[BIOS]** をクリックします。
3. 右側のパネルで、**[Smart Card BIOS Password Properties]**（スマート カードの BIOS パスワードのプロパティ）の**[Settings]**（設定）をクリックします。
4. リブート時に PIN を要求するには、該当のチェック ボックスにチェックを入れます。

注記　この要件を削除するには、このチェック ボックスのチェックを外します。

5. スマート カードの PIN を入力して**[OK]**をクリックします。

スマート カード リーダーの選択

スマート カードを使用する前に、スマート カード セキュリティで正しいスマート カード リーダーが選択されていることを確認してください。スマート カード セキュリティで正しいリーダーが選択されていないと、一部の機能が使用できなくなるか、正しく表示されない場合があります。

スマート カード リーダーを選択するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Smart Card Security]**（スマート カード セキュリティ）をクリックし、**[General]**（全般）をクリックします。
3. 右側のパネルの**[Smart Card Reader]**（スマート カード リーダー）で正しいリーダーをクリックします。
4. スマート カードをリーダーに挿入します。リーダーの情報が自動的に更新されます。

スマート カードの PIN の変更

スマート カードの PIN を変更するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Smart Card Security]**（スマート カード セキュリティ）をクリックし、**[Smart Card]**（スマート カード）をクリックします。
3. 右側のパネルで、**[Change PIN]**（PIN の変更）の**[Change PIN]**をクリックします。
4. 現在のスマート カードの PIN を入力します。
5. 新しい PIN を設定して確定します。
6. 確認ダイアログ ボックスで**[OK]**をクリックします。

スマート カードのバックアップと復元

スマート カードを初期化し、そのカードが使用できるようになったら、スマート カード リカバリ ファイルを作成することを強くおすすめします。リカバリ ファイルを使用すると、スマート カード データをあるスマート カードから別のスマート カードに転送できます。また、このファイルは元のスマート カードのバックアップや、スマート カードが紛失したり盗まれたりしたときのデータの復元にも使用できます。

注意　保管しているリカバリ ファイルと、情報が更新されたスマート カードとの間に不一致が生じないように、新しいリカバリ ファイルを直ちに作成し、安全な場所に保管してください。バックアップ スマート カードがある場合は、新しいリカバリ ファイルをバックアップ スマート カードに復元して、バックアップ スマート カード上の情報も更新する必要があります。

リカバリ ファイルの作成

リカバリ ファイルを作成するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Smart Card Security]**（スマート カード セキュリティ）をクリックし、**[Smart Card]**（スマート カード）をクリックします。
3. 右側のパネルで、**[Recovery]**（リカバリ）の**[Create]**（作成）をクリックします。
4. スマート カードの PIN を入力して**[OK]**をクリックします。
5. **[Filename]**（ファイル名）ボックスに、ファイル パスとファイル名を入力します。

   注意　コンピュータにアクセスできなくなることを防ぐため、リカバリ ファイルをコンピュータのハードドライブには保存しないでください。スマート カードがないと、このファイルにもアクセスできなくなります。また、リカバリ ファイルをハードドライブに保存すると第三者からアクセスされる可能性もあるため、セキュリティ上の危険にさらされます。

6. リカバリ ファイルのパスワードを設定して確定し、**[OK]**をクリックします。

注意　スマート カード リカバリ ファイルのデータが失われることを防ぐため、リカバリ ファイルのパスワードを忘れないようにしてください。パスワードを忘れると、リカバリ ファイルからカードを再作成できなくなります。

スマート カード データの復元

リカバリ ファイルからスマート カード データを復元できます。この機能は、カードが紛失したり盗まれたりした場合や、バックアップ スマート カードを作成する場合に特に有効です。以前のデータが保存されているカードを使用した場合は、そのデータに上書きされます。

開始する前に、以下のものを用意する必要があります。

- スマート カード セキュリティ ソフトウェアがインストールされている、アクセス可能なコンピュータ
- スマート カード リカバリ ファイル
- スマート カード リカバリ ファイルのパスワード
- スマート カード

スマート カードを復元するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Smart Card Security]**（スマート カード セキュリティ）をクリックし、**[Smart Card]**（スマート カード）をクリックします。
3. スマート カード リカバリ ファイルが含まれているフロッピーディスクまたは他のメディアを挿入します。
4. スマート カードをリーダーに挿入します。カードが初期化されていない場合は、初期化するよう要求されます。スマート カードの初期化の詳しい手順については、この章の「スマート カードの初期化」を参照してください。
5. 右側のパネルで、**[Recovery]**（リカバリ）の**[Restore]**（復元）をクリックします。
6. 正しいリカバリ ファイル名が選択されていることを確認し、リカバリ ファイルのパスワードを入力します。
7. スマート カードの PIN を入力します。
8. **[OK]**をクリックします。新しいスマート カードに、元のスマート カードの内容が復元されます。

バックアップ スマート カードの作成

バックアップのために、スマート カードを複製することを強くおすすめします。スマート カード パスワードを手動で生成したか、ランダムに生成したかによって、次の 2 つの作成方法のどちらかを実行します。

ランダムに生成されたスマート カード パスワードを使用して代替スマート カードを作成するには、次の操作を行います。

▲ スマート カードをリーダーに挿入し、そのスマート カードに適切なリカバリ ファイルをロードします。詳しくは、この章の「スマート カード データの復元」を参照してください。

手動で生成したスマート カード パスワードを使用して代替スマート カードを作成するには、以下の手順で操作します。

1. 新しいスマート カードを初期化します。手順については、この章の「スマート カードの初期化」を参照してください。
2. 新しいスマート カードに管理者カードまたはユーザ カードのパスワードを格納します。手順については、この章の「管理者カードまたはユーザ カードのパスワードの格納」を参照してください。

3 Java Card Security for HP ProtectTools

Java Card Security for HP ProtectTools は、オプションのスマート カード リーダーが装備されたコンピュータでの Java Card のセットアップおよび設定を管理します。

Java Card Security for ProtectTools を使用すると、次のことができます。

- Java Card のセキュリティ機能にアクセスできます。
- [Computer Setup]ユーティリティを使用して電源投入時の環境で Java Card の認証を可能にし、また Java Card を管理者用とユーザ用に分けて設定できます。これにより、オペレーティング システムをロードさせるには、ユーザが Java Card を挿入し PIN を入力することが必要となります。
- Java Card のユーザ認証を行うための PIN の設定および変更を行えます。
- Java Card の電源投入時認証データのバックアップおよびリストア（復元）を行えます。

一般的なタスク

[General]（全般）ページを使用すると、次のタスクを実行できます。

- Java Card の PIN の変更
- スマート カード リーダーの選択

注記　スマート カード リーダーでは、Java Card とスマート カードの両方を使用します。この機能は、コンピュータに複数のスマート カード リーダーが装備されている場合に使用できます。

Java Card の PIN の変更

Java Card の PIN を変更するには、以下の手順で操作します。

注記　Java Card の PIN は、4 ～ 8 桁の半角数字にする必要があります。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Java Card Security]**（Java Card セキュリティ）をクリックし、**[General]**（全般）をクリックします。
3. PIN が設定されている Java Card をスマート カード リーダーに挿入します。
4. 右側のパネルで、**[Change]**（変更）をクリックします。
5. **[Change PIN]**（PIN の変更）ダイアログ ボックスで、**[Current PIN]**（現在の PIN）ボックスに現在の PIN を入力します。
6. **[New PIN]**（新しい PIN）ボックスに新しい PIN を入力し、**[Confirm New PIN]**（新しい PIN の確認入力）ボックスに PIN を再度入力します。
7. **[OK]**をクリックします。

スマート カード リーダーの選択

Java Card を使用する前に、Java Card Security for ProtectTools で正しいスマート カード リーダーが選択されていることを確認してください。Java Card Security for ProtectTools で正しいリーダーが選択されていないと、一部の機能が使用できなくなるか、正しく表示されない場合があります。

スマート カード リーダーを選択するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Java Card Security]**（Java Card セキュリティ）をクリックし、**[General]**（全般）をクリックします。
3. Java Card をスマート カード リーダーに挿入します。
4. 右側のパネルの**[Smart Card Reader]**（スマート カード リーダー）で正しいリーダーをクリックします。

高度なタスク（管理者のみ）

[Advanced]（アドバンス）ページを使用すると、次のタスクを実行できます。

- Java Card の PIN の割り当て
- Java Card への名前の割り当て
- 電源投入時認証の設定
- Java Card のバックアップおよびリストア（復元）

注記　[Advanced]ページにアクセスするには、[Computer Setup]ユーティリティのセットアップ パスワードが必要です。

Java Card の PIN の割り当て

電源投入時認証に Java Card を使用できるようにするには、Java Card に PIN を割り当てる必要があります。

Java Card の PIN を割り当てるには、以下の手順で操作します。

注記　Java Card の PIN は、4 ～ 8 桁の半角数字にする必要があります。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Java Card Security]**（Java Card セキュリティ）をクリックし、**[General]**（全般）をクリックします。
3. 新しい Java Card をスマート カード リーダーに挿入します。
4. **[Change PIN]**（PIN の変更）ダイアログ ボックスが表示されたら、**[New PIN]**（新しい PIN）ボックスに新しい PIN を入力し、**[Confirm New PIN]**（新しい PIN の確認入力）ボックスに PIN を再度入力します。
5. **[OK]**をクリックします。

Java Card への名前の割り当て

電源投入時認証に Java Card を使用できるようにするには、Java Card に名前を割り当てる必要があります。

Java Card に名前を割り当てるには、以下の手順で操作します。

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Java Card Security]**（Java Card セキュリティ）をクリックし、**[Advanced]**（アドバンス）をクリックします。
3. **[Setup Password]**（セットアップ パスワード）ダイアログ ボックスが表示されたら、[Computer Setup]ユーティリティのセットアップ パスワードを入力して**[OK]**をクリックします。
4. Java Card をスマート カード リーダーに挿入します。

   注記　このカードにまだ PIN を割り当てていない場合は、[Change PIN]（PIN の変更）ダイアログ ボックスが表示され、新しい PIN を入力できるようになります。

5. 右側のパネルで、**[Java Card name]**（Java Card 名）の**[Change]**（変更）をクリックします。
6. **[Name]**（名前）ボックスに、Java Card の名前を入力します。
7. **[PIN]**ボックスに、現在の Java Card の PIN を入力します。
8. **[OK]**をクリックします。

電源投入時認証の設定

電源投入時認証が有効になると、Java Card を使用してコンピュータを起動することが必要になります。

Java Card の電源投入時認証を有効にするプロセスには、以下の手順が含まれます。

1. BIOS Configuration または[Computer Setup]ユーティリティで、Java Card の電源投入時認証サポートを有効にします。「第 5 章 BIOS Configuration for HP ProtectTools」の「スマート カードまたは Java Card の電源投入時認証サポートの有効/無効の設定」を参照してください。
2. Java Card Security for ProtectTools で、Java Card の電源投入時認証を有効にします。この章の「Java Card の電源投入時認証の有効化および管理者 Java Card の作成」を参照してください。
3. 管理者 Java Card を作成し、有効にします。

Java Card の電源投入時認証の有効化および管理者 Java Card の作成

Java Card の電源投入時認証を有効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Java Card Security]**（Java Card セキュリティ）をクリックし、**[Advanced]**（アドバンス）をクリックします。
3. **[Computer Setup Password]**（[Computer Setup]のパスワード）ダイアログ ボックスが表示されたら、[Computer Setup]ユーティリティのセットアップ パスワードを入力して**[OK]**をクリックします。
4. Java Card をスマート カード リーダーに挿入します。

   注記　このカードにまだ PIN を割り当てていない場合は、**[Change PIN]**（PIN の変更）ダイアログ ボックスが表示され、新しい PIN を入力できるようになります。

5. 右側のパネルで、**[Power-on authentication]**（電源投入時認証）の**[Enable]**（有効にする）チェック ボックスにチェックを入れます。
6. DriveLock をまだ有効にしていない場合は、Java Card の PIN を入力して**[OK]**をクリックします。

   または

   DriveLock をすでに有効にしている場合は、以下の手順で操作します。

   a. **[Make Java card identity unique]**（独自の Java card の ID を作成する）をクリックします。

      または

      [Make the Java card identity the same as the DriveLock password]（Java card の ID を DriveLock のパスワードと同じにする）をクリックします。

      注記　コンピュータで DriveLock が有効になっていると、Java Card の ID を DriveLock の user password（ユーザ パスワード）と同じものに設定できます。これにより、コンピュータを起動するときに、Java Card のみを使用して DriveLock と Java Card の両方を検証できるようになります。

   b. 必要に応じて、**[DriveLock password]**（DriveLock パスワード）ボックスに DriveLock の user password（ユーザ パスワード）を入力し、**[Confirm password]**（パスワードの確認）ボックスにパスワードを再度入力します。

   c. Java Card の PIN を入力します。

   d. **[OK]**をクリックします。

7. リカバリ ファイルを作成するよう要求されたら、「リカバリ ファイルの作成」を参照するか、または**[Cancel]**（キャンセル）をクリックして後でリカバリ ファイルを作成することもできます。

ユーザ Java Card の作成

注記　ユーザ Java Card を作成するには、電源投入時認証および管理者カードが設定されている必要があります。

ユーザ Java Card を作成するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Java Card Security]**（Java Card セキュリティ）をクリックし、**[Advanced]**（アドバンス）をクリックします。
3. **[Setup Password]**（セットアップ パスワード）ダイアログ ボックスが表示されたら、[Computer Setup]ユーティリティのセットアップ パスワードを入力して**[OK]**をクリックします。
4. ユーザ カードとして使用する Java Card を挿入します。
5. 右側のパネルで、**[Power-on authentication]**（電源投入時認証）の**[User card identity]**（ユーザ カードの ID）の横にある**[Create]**（作成）をクリックします。
6. ユーザ Java Card の PIN を入力して[OK]をクリックします。

Java Card の電源投入時認証の無効化

Java Card の電源投入時認証を無効にすると、コンピュータにアクセスするために Java Card を使用する必要はなくなります。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Java Card Security]**（Java Card セキュリティ）をクリックし、**[Advanced]**（アドバンス）をクリックします。
3. **[Setup Password]**（セットアップ パスワード）ダイアログ ボックスが表示されたら、[Computer Setup]ユーティリティのセットアップ パスワードを入力して**[OK]**をクリックします。
4. Java Card を挿入し、PIN を入力して**[OK]**をクリックします。
5. 右側のパネルで、**[Power-on authentication]**（電源投入時認証）の**[Enable]**（有効にする）チェック ボックスのチェックを外します。

Java Card のバックアップと復元

Java Card に電源投入時認証 ID を割り当てたら、Java Card リカバリ ファイルを作成することを強くおすすめします。リカバリ ファイルを使用すると、Java Card の電源投入時認証 ID データを、ある Java Card から別の Java Card に転送できます。また、このファイルは、元の Java Card のバックアップや、Java Card が紛失したり盗まれたりしたときのデータの復元にも使用できます。

注意　保管しているリカバリ ファイルと、情報が更新された Java Card との間に不一致が生じないように、直ちにリムーバブル メディアに新しいリカバリ ファイルを作成し、安全な場所に保管してください。バックアップ Java Card がある場合は、新しいリカバリ ファイルをバックアップ Java Card に復元して、バックアップ Java Card 上の情報も更新する必要があります。

リカバリ ファイルの作成

リカバリ ファイルを作成するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Java Card Security]**（Java Card セキュリティ）をクリックし、**[Advanced]**（アドバンス）をクリックします。
3. **[Setup Password]**（セットアップ パスワード）ダイアログ ボックスが表示されたら、[Computer Setup]ユーティリティのセットアップ パスワードを入力して**[OK]**をクリックします。
4. 右側のパネルで、**[Recovery]**（リカバリ）の**[Create]**（作成）をクリックします。
5. **[Filename]**（ファイル名）ボックスに、ファイル パスとファイル名を入力します。

   注意　コンピュータにアクセスできなくなることを防ぐため、リカバリ ファイルをコンピュータのハードドライブには保存しないでください。Java Card がないと、このファイルにもアクセスできなくなります。また、リカバリ ファイルをハードドライブに保存すると第三者からアクセスされる可能性もあるため、セキュリティ上の危険にさらされます。

6. **[Recovery file password]**（リカバリ ファイルのパスワード）ボックスにリカバリ ファイルのパスワードを入力し、**[Confirm password]**（パスワードの確認）ボックスにパスワードを再度入力します。
7. Java Card の PIN を入力して**[OK]**をクリックします。

注意　Java Card リカバリ ファイルのデータが失われることを防ぐため、リカバリ ファイルのパスワードを忘れないようにしてください。パスワードを忘れると、リカバリ ファイルからカードを再作成できなくなります。

Java Card データの復元

リカバリ ファイルから Java Card データを復元できます。この機能は、カードが紛失したり盗まれたりした場合や、バックアップ Java Card を作成する場合に特に有効です。以前のデータが保存されているカードを使用した場合は、そのデータに上書きされます。

開始する前に、以下のものを用意する必要があります。

- Java Card Security for ProtectTools ソフトウェアがインストールされている、アクセス可能なコンピュータ
- Java Card リカバリ ファイル
- Java Card リカバリ ファイルのパスワード
- Java Card

Java Card を復元するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Java Card Security]**（Java Card セキュリティ）をクリックし、**[Advanced]**（アドバンス）をクリックします。
3. **[Setup Password]**（セットアップ パスワード）ダイアログ ボックスが表示されたら、[Computer Setup]ユーティリティのセットアップ パスワードを入力して**[OK]**をクリックします。
4. Java Card リカバリ ファイルが含まれているフロッピーディスクまたは他のメディアを挿入します。
5. Java Card をリーダーに挿入します。カードに PIN が割り当てられていない場合は、PIN を作成するよう要求されます。Java Card に PIN を割り当てるための詳しい手順については、この章の「Java Card の PIN の割り当て」を参照してください。
6. 右側のパネルで、[Recovery]（リカバリ）の**[Restore]**（復元）をクリックします。
7. 正しいリカバリ ファイル名が選択されていることを確認し、リカバリ ファイルのパスワードを入力します。
8. Java Card の PIN を入力します。
9. **[OK]**をクリックします。

   新しい Java Card に、元の Java Card の内容が復元されます。

バックアップ Java Card の作成

バックアップのために、Java Card を複製することを強くおすすめします。

代替 Java Card を作成するには、次の操作を行います。

▲ Java Card をリーダーに挿入し、その Java Card に適切なリカバリ ファイルをロードします。詳しくは、この章の「Java Card データの復元」を参照してください。

4 Embedded Security for HP ProtectTools

注記 Embedded Security for HP ProtectTools を使用するには、統合された TPM（Trusted Platform Module）セキュリティ チップがコンピュータに内蔵されている必要があります。

Embedded Security for HP ProtectTools は、ユーザ データや証明書を不正なアクセスから保護します。このソフトウェア モジュールには、以下のセキュリティ機能があります。

- 高度な Microsoft EFS（Encryption File System）ファイルおよびフォルダの暗号化
- ユーザ データを保護するための PSD（Personal Secure Drive）の作成
- データ管理機能（キー階層のバックアップや復元など）
- Embedded Security ソフトウェアの使用時にデジタル証明書の操作を保護する、他社製のアプリケーション（Microsoft® Outlook や Internet Explorer など）のサポート

TPM 内蔵セキュリティ チップを使用すると、HP ProtectTools セキュリティマネージャの他のセキュリティ機能を強化したり有効にしたりできます。たとえば、Credential Manager for HP ProtectTools では、内蔵チップを Windows へのログオン時の認証要素として使用できます。一部のモデルでは、TPM 内蔵セキュリティ チップを使用して、BIOS Configuration for HP ProtectTools からアクセスする高度な BIOS セキュリティ機能を有効にすることもできます。

セットアップ手順

注意　セキュリティ上の危険にさらされないようにするために、IT 管理者が内蔵セキュリティ チップを直ちに初期化することを強くおすすめします。内蔵セキュリティ チップを初期化しない場合、不正なユーザ、コンピュータ ワーム、またはウィルスがコンピュータのオーナシップを奪い、緊急リカバリ アーカイブの処理やユーザ アクセスの設定など所有者のタスクを制御してしまう可能性があります。

以下の 2 つの項目の手順に従い、内蔵セキュリティ チップを有効にして初期化します。

内蔵セキュリティ チップの有効化

内蔵セキュリティ チップは、[Computer Setup]ユーティリティで有効にする必要があります。この手順は、BIOS Configuration for HP ProtectTools では実行できません。

内蔵セキュリティ チップを有効にするには、以下の手順で操作します。

1. コンピュータの電源を入れるか再起動し、画面の左下隅に[F10 = ROM Based Setup]（ROM ベースのセットアップ）というメッセージが表示されている間に F10 キーを押して、[Computer Setup]を起動します。
2. 管理者パスワードを設定していない場合は、矢印キーを使用して**[Security]**（セキュリティ設定）→**[Setup password]**（セットアップ パスワード）の順に選択して enter キーを押します。
3. **[New password]**（新しいパスワード）および**[Verify new password]**（新しいパスワードの確認）ボックスにパスワードを入力して f10 キーを押します。
4. **[Security]**（セキュリティ設定）メニューで、矢印キーを使用して**[TPM Embedded Security]**（TPM 内蔵セキュリティ）を選択し、enter キーを押します。
5. **[Embedded Security]**（内蔵セキュリティ）にデバイスが表示されない場合、**[Available]**（利用可能）を選択します。
6. **[Embedded security device state]**（内蔵セキュリティ デバイスの状態）を選択し、**[Enable]**（有効にする）に変更します。
7. f10 キーを押して、Embedded Security の設定への変更を確定します。
8. 設定を保存して[Computer Setup]を終了するには、矢印キーを使用して**[File]**（ファイル）→**[Save changes and exit]**（設定を保存して終了）の順に選択します。次に、画面の説明に沿って操作します。

内蔵セキュリティ チップの初期化

内蔵セキュリティの初期化プロセスでは、以下のことを行います。

- 内蔵セキュリティ チップ上のすべての所有者機能へのアクセスを保護する、内蔵セキュリティ チップの所有者のパスワードを設定します。
- すべてのユーザの基本ユーザ キーを再暗号化できるようにするための保護された記憶域である、緊急リカバリ アーカイブをセットアップします。

内蔵セキュリティ チップを初期化するには、以下の手順で操作します。

1. タスク バーの右端の通知領域にある[HP ProtectTools Security Manager]（HP ProtectTools セキュリティ マネージャ）アイコンを右クリックして、**[Embedded Security Initialization]**（内蔵セキュリティの初期化）を選択します。

   [HP ProtectTools Embedded Security Initialization Wizard]（HP ProtectTools Embedded Security 初期化ウィザード）が起動します。

2. **[Next]**（次へ）をクリックします。
3. 所有者のパスワードを設定して確定し、**[Next]**をクリックします。

   [Setup Emergency Recovery]（緊急リカバリのセットアップ）ダイアログ ボックスが表示されます。

4. **[Next]**をクリックしてリカバリ アーカイブのデフォルトの場所を受け入れるか、または**[Browse]**（参照）ボタンをクリックして別の場所を選択し、**[Next]**をクリックします。
5. 緊急リカバリ トークンのパスワードを設定して確定し、**[Next]**をクリックします。
6. **[Browse]**（参照）をクリックし、緊急リカバリ アーカイブの場所を選択して**[Next]**（次へ）をクリックします。
7. [Summary]（サマリー）ページで**[Next]**をクリックします。
   - この時点で基本ユーザ アカウントをセットアップしない場合は、**[Start the Embedded Security User Initialization Wizard]**（Embedded Security ユーザ初期化ウィザードを開始する）チェック ボックスのチェックを外して**[Finish]**（完了）をクリックします。次の項目の指示に従うと、ウィザードをいつでも手動で起動して基本ユーザ アカウントをセットアップできます。
   - 基本ユーザ アカウントをセットアップする場合は、**[Start the Embedded Security User Initialization Wizard]**チェック ボックスにチェックを入れ、**[Finish]**をクリックします。[Embedded Security User Initialization Wizard]（Embedded Security ユーザ初期化ウィザード）が起動します。詳しくは、次の項目の手順を参照してください。

基本ユーザ アカウントのセットアップ

Embedded Security で基本ユーザ アカウントをセットアップすると、次のようになります。

- 暗号化された情報を保護するための基本ユーザ キーが生成され、その基本ユーザ キーを保護する基本ユーザ キーのパスワードが設定されます。
- 暗号化されたファイルおよびフォルダを格納するための PSD（Personal Secure Drive）が設定されます。

注意　基本ユーザ キーのパスワードを保護してください。このパスワードがないと、暗号化されたデータにアクセスしたり復元したりできなくなります。

基本ユーザ アカウントをセットアップしてユーザ セキュリティ機能を有効にするには、以下の手順で操作します。

1. [Embedded Security User Initialization Wizard]（Embedded Security ユーザ初期化ウィザード）が起動していない場合は、**[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[User Settings]**（ユーザーの設定）の順にクリックします。
3. 右側のパネルで、**[Embedded Security Features]**（内蔵セキュリティの機能）の**[Configure]**（設定）をクリックします。

   [Embedded Security User Initialization Wizard]（Embedded Security ユーザ初期化ウィザード）が起動します。
4. **[Next]**（次へ）をクリックします。
5. 基本ユーザ キーのパスワードを設定して確定し、**[Next]**をクリックします。
6. **[Next]**をクリックして設定を確定します。
7. 必要なセキュリティ機能を選択して**[Next]**をクリックします。
8. **[Next]**を再度クリックします。

   注記　セキュリティ保護された電子メールを使用するには、最初に、Embedded Security で作成されたデジタル証明書を使用するように電子メール クライアントを設定する必要があります。デジタル証明書が使用できない場合は、証明機関から取得する必要があります。電子メールを設定してデジタル証明書を取得する手順については、電子メール クライアントのヘルプを参照してください。
9. 複数の暗号化証明書が存在する場合は、適切な証明書を選択して**[Next]**をクリックします。
10. PSD のドライブ文字とラベルを選択して**[Next]**をクリックします。
11. PSD のサイズと場所を選択して**[Next]**をクリックします。
12. [Summary]（サマリー）ページで**[Next]**をクリックします。
13. **[Finish]**（完了）をクリックします。

一般的なタスク

基本ユーザ アカウントのセットアップを完了すると、以下のタスクを実行できます。

- ファイルおよびフォルダの暗号化
- 暗号化された電子メールの送受信

Personal Secure Drive の使用

PSD のセットアップを完了すると、次回のログオンで、基本ユーザ キーのパスワードを入力するよう要求されます。基本ユーザ キーのパスワードを正しく入力すると、Windows エクスプローラから直接 PSD にアクセスできます。

ファイルおよびフォルダの暗号化

暗号化ファイルを操作する場合は、以下の規則を考慮してください。

- 暗号化できるファイルおよびフォルダは、NTFS パーティション上のものだけです。FAT パーティション上のファイルおよびフォルダは暗号化できません。
- システム ファイルや圧縮されたファイルは暗号化できません。また、暗号化されたファイルは圧縮できません。
- 一時フォルダは、ハッカーの関心を引く可能性があるため、暗号化するようにしてください。
- ファイルまたはフォルダを初めて暗号化した時、回復ポリシーが自動的にセットアップされます。暗号化証明書や秘密キーをなくした場合でも、このポリシーによって、回復エージェントを使用して情報の暗号化を解除できるようになります。

ファイルおよびフォルダを暗号化するには、以下の手順で操作します。

1. 暗号化するファイルまたはフォルダを右クリックします。
2. **[Encrypt]**（暗号化）をクリックします。
3. 以下のオプションのどちらかをクリックします。
   - **[[Apply changes to this folder only]（このフォルダにのみ変更を適用する）]**
   - **[[Apply changes to this folder, subfolders, and files]（このフォルダ、およびサブフォルダとファイルに変更を適用する）]**
4. **[OK]**をクリックします。

暗号化された電子メールの送受信

Embedded Security では、暗号化された電子メールの送受信を行うことができますが、その手順は電子メールのアクセスに使用しているプログラムによって異なります。詳しくは、Embedded Security のヘルプおよび使用している電子メール アプリケーションのヘルプを参照してください。

基本ユーザ キーのパスワードの変更

基本ユーザ キーのパスワードを変更するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[User Settings]**（ユーザーの設定）の順にクリックします。
3. 右側のパネルで、**[Basic User Key password]**（基本ユーザ キーのパスワード）の**[Change]**（変更）をクリックします。
4. 古いパスワードを入力した後、新しいパスワードを設定して確定します。
5. **[OK]**をクリックします。

高度なタスク

バックアップと復元

Embedded Security のバックアップ機能では、緊急の場合に復元される証明情報を含むアーカイブが作成されます。

バックアップ ファイルの作成

バックアップ ファイルを作成するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[Backup]**（バックアップ）の順にクリックします。
3. 右側のパネルで、**[Backup]**をクリックします。
4. **[Browse]**（参照）をクリックして、バックアップ ファイルを保存する場所を選択します。
5. バックアップ情報に緊急リカバリ アーカイブを追加するかどうかを選択します。
6. **[Next]**（次へ）をクリックします。
7. **[Finish]**（完了）をクリックします。

バックアップ ファイルからの証明データの復元

バックアップ ファイルからデータを復元するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[Backup]**（バックアップ）の順にクリックします。
3. 右側のパネルで、**[Restore]**（復元）をクリックします。
4. **[Browse]**（参照）をクリックして、格納された場所からバックアップ ファイルを選択します。
5. **[Next]**（次へ）をクリックします。
6. [Embedded Security User Initialization Wizard]（Embedded Security ユーザ初期化ウィザード）を開始するかどうかを選択します。
   - ウィザードを開始する場合は、[Finish]（完了）をクリックし、画面の説明に沿って初期化を完了します。詳しくは、この章の「基本ユーザ アカウントのセットアップ」を参照してください。
   - ウィザードを開始しない場合は、**[Finish]**をクリックします。

所有者のパスワードの変更

所有者のパスワードを変更するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[Advanced]**（アドバンス）の順にクリックします。
3. 右側のパネルで、**[Owner Password]**（所有者のパスワード）の**[Change]**（変更）をクリックします。
4. 古い所有者のパスワードを入力した後、新しい所有者のパスワードを設定して確定します。
5. **[OK]**をクリックします。

ユーザ パスワードの再設定

ユーザが忘れたパスワードを管理者により再設定してもらうことができます。詳しくは、ヘルプを参照してください。

Embedded Security の有効化と無効化

セキュリティ機能を使用しないで操作する場合は、Embedded Security の機能を無効にすることができます。

Embedded Security の機能は、次の 2 種類のレベルで有効または無効にすることができます。

- 一時的な無効化：このオプションを使用すると、Windows の再起動時に Embedded Security が自動的に再び有効になります。このオプションは、初期設定ですべてのユーザが使用できます。
- 永続的な無効化：このオプションを使用すると、Embedded Security を再び有効にするには所有者のパスワードが必要になります。このオプションは、管理者だけが使用できます。

Embedded Security の永続的な無効化

Embedded Security を永続的に無効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[Advanced]**（アドバンス）の順にクリックします。
3. 右側のパネルで、**[Embedded Security]**の**[Disable]**（無効にする）をクリックします。
4. プロンプトで所有者のパスワードを入力して**[OK]**をクリックします。

Embedded Security の永続的な無効化の後の有効化

Embedded Security を永続的に無効にした後で再び有効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[Advanced]**（アドバンス）の順にクリックします。

3. 右側のパネルで、**[Embedded Security]**の**[Enable]**（有効にする）をクリックします。

4. プロンプトで所有者のパスワードを入力して**[OK]**をクリックします。

移行ウィザードによるキーの移行

移行は、キーや証明書の管理、復元、転送などを行うことができる、高度な管理者タスクです。

移行について詳しくは、Embedded Security のヘルプを参照してください。

5 BIOS Configuration for HP ProtectTools

BIOS Configuration for HP ProtectTools を使用すると、[Computer Setup]ユーティリティのセキュリティ設定にアクセスできます。これにより、[Computer Setup]で管理されるシステムのセキュリティ機能に Windows から簡単にアクセスできるようになります。

BIOS Configuration を使用すると、次のことができます。

- 電源投入時パスワードおよび管理者パスワードを管理できます。
- スマート カード パスワードおよび内蔵セキュリティ認証サポートの有効化など、電源投入時のその他の認証機能を設定できます。
- CD-ROM のブートや各種ハードウェア ポートなど、ハードウェア機能を有効または無効に設定できます。
- マルチブートの有効化および起動順序の変更を含む、ブート オプションを設定できます。

注記 BIOS Configuration for HP ProtectTools にある機能の多くは、[Computer Setup]でも使用できます。

一般的なタスク

BIOS Configuration を使用すると、通常は起動時に f10 キーを押して[Computer Setup]を使用することでしかアクセスできない、各種のコンピュータ設定を管理できます。

ブート オプションの管理

BIOS Configuration を使用すると、コンピュータの起動や再起動に実行されるタスクに対する各種の設定を管理できます。

ブート オプションを管理するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）をクリックします。
3. BIOS の管理者パスワードのプロンプトで[Computer Setup]の管理者パスワードを入力して、**[OK]**をクリックします。

注記　BIOS の管理者パスワードのプロンプトは、[Computer Setup]のセットアップ パスワードがすでに設定されている場合だけ表示されます。[Computer Setup]のセットアップ パスワードの設定について詳しくは、この章の「セットアップ パスワードの設定」を参照してください。

4. 左側のパネルで、**[System Configuration]**（システム コンフィギュレーション）をクリックします。
5. 右側のパネルで、f9、f10、および f12 と、**[Express Boot Popup Delay（Sec）]**（高速ブート ポップアップ遅延（秒））に対する遅延時間（秒単位）を選択します。
6. **[MultiBoot]**（マルチブート）を有効または無効にします。
7. マルチブートを有効にしている場合は、ブート デバイスを選択し、上向きの矢印または下向きの矢印をクリックして一覧内の順序を調整することで、起動順序を選択します。
8. **[Apply]**（適用）をクリックし、[HP ProtectTools]ウィンドウで**[OK]**をクリックして変更を保存します。

システム コンフィギュレーション オプションの有効/無効の設定

注記　次の項目の一部は、お使いのコンピュータでサポートされていない場合があります。

デバイスまたはセキュリティ オプションの有効/無効を切り替えるには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）をクリックします。
3. BIOS の管理者パスワードのプロンプトで[Computer Setup]の管理者パスワードを入力して、**[OK]**をクリックします。
4. 左側のパネルで**[System Configuration]**（システム コンフィギュレーション）をクリックしてから、以下のシステム コンフィギュレーション オプションの有効/無効を切り替えるか、右側のパネルでオプションの設定を行います。
   - Port Options（ポート オプション）
     - Serial Port（シリアル ポート）
     - Infared Port（赤外線ポート）
     - Parallel Port（パラレル ポート）
     - SD Slot（SD スロット）
     - USB Port（USB ポート）
     - 1394 Port（1394 ポート）
     - Cardbus Slot（カードバス スロット）
     - ExpressCard slot（ExpressCard スロット）
   - Boot Options（ブート オプション）
     - f9, f10, and f12 Delay (Sec)（f9、f10、および f12 の遅延（秒））
     - MultiBoot（マルチブート）
     - Express Boot Popup Delay (Sec)（高速ブート ポップアップ遅延（秒））
     - CD-ROM Boot（CD-ROM ドライブからのブート）
     - Floppy Boot（フロッピーディスク ドライブからのブート）
     - Internal Network Adapter Boot（内蔵ネットワーク アダプタ ブート）
     - Internal Network Adapter Boot Mode (PXE or RPL)（内蔵ネットワーク アダプタ ブート モード（PXE または RPL））
     - Boot Order（ブート順序）
   - Device Configurations（デバイス設定）
     - NumLock at Boot（ブート時 NumLock）
     - Swapping fn/ctrl Keys（[fn]/[ctrl]キーの切り替え）

- Multiple Pointing Devices（マルチポインティング デバイス）
- USB Legacy Support（USB レガシー サポート）
- Parallel port mode (standard, bidirectional, EPP, or ECP)（パラレル ポート モード：EPP（Enhanced Parallel Port）、標準、双方向、または ECP（Enhanced Capabilities Port））
- Data Execution Prevention（データ実行防止）
- SATA Native Mode（SATA ネイティブ モード）
- Dual Core CPU（デュアル コア CPU）
- Automatic Intel® SpeedStep Functionality Support（Automatic Intel SpeedStep 機能サポート）
- Fan Always on While on AC Power（外部電源の使用中は常にファンをオンにする）
- BIOS DMA Data Transfers（BIOS ATA DMA 転送）
- Intel or AMD PSAE Execution Disable（Intel または AMD PSAE の実行無効設定）

● Built-In Device Options（内蔵デバイス オプション）

- Embedded WLAN Device Radio（内蔵無線 LAN デバイスの無線）
- Embedded WWAN Device Radio（内蔵無線 WAN デバイスの無線）
- Embedded Bluetooth® Device Radio（内蔵 Bluetooth デバイスの無線）
- LAN/WLAN Switching（LAN/無線 LAN の切り替え）
- Wake on LAN from Off（電源オフ状態からの Wake on LAN の実行）

5. **[Apply]**（適用）をクリックし、[HP ProtectTools]ウィンドウで**[OK]**をクリックして変更を保存してから終了します。

高度なタスク

HP ProtectTools の設定の管理

HP ProtectTools セキュリティ マネージャの一部の機能は、BIOS Configuration で管理できます。

スマート カードまたは Java Card の電源投入時認証サポートの有効/無効の設定

このオプションを有効にすると、スマート カードまたは Java Card をコンピュータの電源投入時のユーザ認証に使用できます。

注記　電源投入時認証機能を完全に有効にするには、Smart Card Security for HP ProtectTools モジュールまたは Java Card Security for HP ProtectTools モジュールを使用してスマート カードを設定する必要もあります。

スマート カードの電源投入時認証サポートを有効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）をクリックします。
3. BIOS の管理者パスワードのプロンプトで[Computer Setup]の管理者パスワードを入力して、**[OK]** をクリックします。
4. 左側のパネルで、**[Security]**（セキュリティ）をクリックします。
5. **[Smart Card Security]**（スマート カード セキュリティ）で、**[Enable]**（有効にする）をクリックします。

   注記　スマート カード電源投入時認証を無効にするには、**[Disable]**（無効にする）をクリックします。

6. **[Apply]**（適用）をクリックし、[HP ProtectTools]ウィンドウで**[OK]**をクリックして変更を保存します。

内蔵セキュリティの電源投入時認証サポートの有効/無効の設定

このオプションを有効にすると、TPM 内蔵セキュリティ チップ（使用可能な場合のみ）をコンピュータの電源投入時のユーザ認証に使用できます。

注記　電源投入時認証機能を完全に有効にするには、Embedded Security for HP ProtectTools モジュールを使用して TPM 内蔵セキュリティ チップを設定する必要もあります。

内蔵セキュリティの電源投入時認証サポートを有効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）をクリックします。
3. BIOS の管理者パスワードのプロンプトで[Computer Setup]の管理者パスワードを入力して、**[OK]**をクリックします。
4. 左側のパネルで、**[Security]**（セキュリティ）をクリックします。
5. **[Embedded Security]**（内蔵セキュリティ）で、**[Power-on Authentication Support]**（電源投入時認証サポート）の隣の**[Enable]**（有効にする）をクリックします。

   注記　内蔵セキュリティの電源投入時認証を無効にするには、**[Disable]**（無効にする）をクリックします。
6. **[Apply]**（適用）をクリックし、[HP ProtectTools]ウィンドウで**[OK]**をクリックして変更を保存します。

自動 DriveLock によるハードドライブのプロテクトの有効/無効の設定

このオプションが有効になっていると、DriveLock パスワードがドライブ内で自動的に生成および設定され、TPM 内蔵セキュリティ チップによって保護されます。

注記　コンピュータを再起動し、パスワードのプロンプトで正しい TPM 内蔵セキュリティ パスワードを入力するまでは、自動的に生成されたパスワードは設定されません。

自動 DriveLock を有効にするオプションは、以下の条件が満たされていないと使用できません。

- TPM セキュリティ チップがコンピュータに内蔵され、初期化されていること。TPM セキュリティ チップを有効にして初期化する手順については、「第 4 章 Embedded Security for HP ProtectTools」の「内蔵セキュリティ チップの有効化」と「内蔵セキュリティ チップの初期化」を参照してください。
- DriveLock パスワードがまだ有効になっていないこと

注記　コンピュータに DriveLock パスワードがすでに手動で設定されている場合は、自動 DriveLock によるプロテクトを有効にする前に、まず設定されているパスワードを無効にする必要があります。

自動 DriveLock によるプロテクトを有効または無効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）をクリックします。
3. BIOS の管理者パスワードのプロンプトで[Computer Setup]の管理者パスワードを入力して、**[OK]**をクリックします。
4. 左側のパネルで、**[Security]**（セキュリティ）をクリックします。
5. **[Embedded Security]**（内蔵セキュリティ）で、**[Automatic DriveLock Suport]**（自動ドライブロック サポート）の隣の**[Enable]**（有効にする）をクリックします。

   注記　Embedded Security の自動 DriveLock プロテクトを無効にするには、**[Disable]**（無効にする）をクリックします。
6. **[Apply]**（適用）をクリックし、[HP ProtectTools]ウィンドウで**[OK]**をクリックして変更を保存します。

[Computer Setup]のパスワードの管理

BIOS Configuration を使用すると、[Computer Setup]の電源投入時パスワードやセットアップ パスワードの設定および変更を行うことができるほか、各種のパスワード設定も管理できます。

注意　BIOS Configuration の[Passwords]（パスワード）ページで設定したパスワードは、[HP ProtectTools]ウィンドウの**[Apply]**（適用）または**[OK]**ボタンをクリックすると直ちに保存されます。パスワード設定を元に戻す場合も以前のパスワードを指定する必要があるため、設定したパスワードを忘れないようにしてください。

電源投入時パスワードは、ノートブック コンピュータを不正な使用から保護できます。

注記 電源投入時パスワードを設定すると、[Passwords]ページの[Set]（設定）ボタンが[Change]（変更）ボタンに置き換えられます。

[Computer Setup]のセットアップ パスワードは、[Computer Setup]内の設定値とシステム識別情報を保護します。いったんこのパスワードを設定すると、次回から[Computer Setup]で操作するにはパスワードの入力が必要になります。セットアップ パスワードを設定している場合は、HP ProtectTools の BIOS Configuration の部分を起動する前にパスワードを入力するよう要求されます。

注記 セットアップ パスワードを設定すると、[Passwords]ページの[Set]ボタンが[Change]ボタンに置き換えられます。

電源投入時パスワードの設定

電源投入時パスワードを設定するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）→**[Security]**（セキュリティ）の順にクリックします。
3. 右側のパネルで、**[Power-On Password]**（電源投入時パスワード）の隣の**[Set]**（設定）をクリックします。
4. **[Enter Password]**（パスワードの入力）および**[Verify Password]**（パスワードの確認）ボックスにパスワードを入力して確定します。
5. [Passwords]（パスワード）ダイアログ ボックスで**[OK]**をクリックします。
6. **[Apply]**（適用）をクリックし、[HP ProtectTools]ウィンドウで**[OK]**をクリックして変更を保存します。

電源投入時パスワードの変更

電源投入時パスワードを変更するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）→**[Security]**（セキュリティ）の順にクリックします。
3. 右側のパネルで、**[Power-On Password]**（電源投入時パスワード）の隣の**[Change]**（変更）をクリックします。
4. **[Old Password]**（古いパスワード）ボックスに、現在のパスワードを入力します。
5. **[Enter New Password]**（新しいパスワードの入力）ボックスに新しいパスワードを設定して確定します。
6. **[Passwords]**（パスワード）ダイアログ ボックスで**[OK]**をクリックします。
7. **[Apply]**（適用）をクリックし、[HP ProtectTools]ウィンドウで**[OK]**をクリックして変更を保存します。

セットアップ パスワードの設定

[Computer Setup]のセットアップ パスワードを設定するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）→**[Security]**（セキュリティ）の順にクリックします。
3. 右側のパネルで、**[Setup Password]**（セットアップ パスワード）の隣の**[Set]**（設定）を選択します。
4. **[Enter Password]**（パスワードの入力）および**[Confirm Password]**（パスワードの確認）ボックスにパスワードを設定して確定します。
5. **[Passwords]**（パスワード）ダイアログ ボックスで**[OK]**をクリックします。
6. **[Apply]**（適用）をクリックし、[HP ProtectTools]ウィンドウで**[OK]**をクリックして変更を保存します。

セットアップ パスワードの変更

[Computer Setup]のセットアップ パスワードを変更するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）→**[Security]**（セキュリティ）の順にクリックします。
3. 右側のパネルで、**[Setup Password]**（セットアップ パスワード）の隣の**[Change]**（変更）をクリックします。
4. **[Old Password]**（古いパスワード）ボックスに、現在のパスワードを入力します。
5. **[Enter New Password]**（新しいパスワードの入力）および**[Verify new password]**（新しいパスワードの確認）ボックスに新しいパスワードを入力して確定します。
6. **[Passwords]**（パスワード）ダイアログ ボックスで**[OK]**をクリックします。
7. **[Apply]**（適用）をクリックし、[HP ProtectTools]ウィンドウで**[OK]**をクリックして変更を保存します。

パスワード オプションの設定

BIOS Configuration for HP ProtectTools を使用すると、システムのセキュリティを強化するようにパスワード オプションを設定できます。

厳重なセキュリティの有効化と無効化

注意　コンピュータが永久に使用できなくなることを防ぐため、設定したセットアップ パスワード、電源投入時パスワード、またはスマート カードの PIN を、紙などに書いて他人の目にふれない安全な場所に保管しておいてください。これらのパスワードや PIN を忘れてしまうと、コンピュータのロックを解除できなくなります。

厳重なセキュリティを有効にすると、電源投入時パスワード、管理者パスワード、およびその他の電源投入時認証形式による保護が強化されます。

厳重なセキュリティを有効または無効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）→**[Security]**（セキュリティ）の順にクリックします。
3. 右側のパネルの**[Password options]**（パスワード オプション）で、**[Stringent Security]**（厳重なセキュリティ）を有効または無効にします。

   注記　厳重なセキュリティを無効にする場合は、**[Enable Stringent Security]**（厳重なセキュリティの有効化）チェック ボックスのチェックを外します。

4. **[Apply]**（適用）をクリックし、[HP ProtectTools]ウィンドウで**[OK]**をクリックして変更を保存します。

Windows 再起動時の電源投入時認証の有効/無効の設定

このオプションを使用すると、Windows の再起動時にユーザに電源投入時、TPM、またはスマートカードの各パスワードの入力を要求することでセキュリティを強化できます。

Windows の再起動時の電源投入時認証を有効または無効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）→**[Security]**（セキュリティ）の順にクリックします。
3. 右側のパネルの**[Password options]**（パスワード オプション）で、**[Require password on restart]**（再起動時のパスワードの要求）有効または無効にします。
4. **[Apply]**（適用）をクリックし、[HP ProtectTools]ウィンドウで**[OK]**をクリックして変更を保存します。

6 Credential Manager for HP ProtectTools

Credential Manager for HP ProtectTools では、コンピュータへの不正なアクセスに対するセキュリティ機能を提供します。これらのセキュリティ機能には、以下のものが含まれます。

- Windows へのログオン時のパスワードに代わる、スマート カードや指紋認証システムなどを使用した Windows へのログオン。詳しくは、この章の「証明書の登録」を参照してください。
- Web サイト、アプリケーション、および保護されたネットワーク リソースでの証明書を自動的に記憶するシングルサインオン機能
- スマート カードや指紋認証システムなどの、オプションのセキュリティ デバイスのサポート
- コンピュータのロック解除にはオプションのセキュリティ デバイスを使用した認証を必要とするなどの、追加のセキュリティ設定のサポート

セットアップ手順

Credential Manager へのログオン

設定により、以下のどれかの方法で Credential Manager にログオンできます。

- [Credential Manager Logon Wizard]（証明書マネージャ ログオン ウィザード）（推奨）
- 通知領域の[HP ProtectTools Security Manager]（HP ProtectTools セキュリティ マネージャ）アイコン
- HP ProtectTools セキュリティ マネージャ

注記　Windows のログオン画面の Credential Manager ログオン プロンプトを使用して Credential Manager にログオンすると、同時に Windows にもログオンします。

最初に Credential Manager を起動するときは、通常の Windows ログオン パスワードでログオンします。その後、Credential Manager アカウントが、Windows のログオン証明書を使用して自動的に作成されます。

Credential Manager にログオンした後で、指紋やスマート カードなどの、追加の証明書を登録できます。詳しくは、この章の「証明書の登録」を参照してください。

次回のログオン時には、ログオン ポリシーを選択して、登録された証明書の任意の組み合わせを使用することができます。

[Credential Manager Logon Wizard]（証明書マネージャ ログオン ウィザード）の使用

[Credential Manager Logon Wizard]を使用して Credential Manager にログオンするには、以下の手順で操作します。

1. 以下のどれかの方法で[Credential Manager Logon Wizard]を起動します。
   - Windows のログオン画面を使用する
   - 通知領域から、**[HP ProtectTools Security Manager]**アイコンをダブルクリックする
   - ProtectTools セキュリティ マネージャの[Credential Manager]（証明書マネージャ）ページから、ウィンドウの右上隅にある**[Log On]**（ログオン）リンクをクリックする
2. **[Next]**（次へ）をクリックします。
3. **[User name]**（ユーザ名）ボックスにユーザ名を入力します。
4. **[Password]**（パスワード）ボックスにパスワードを入力して**[Next]**をクリックします。
5. **[Finish]**（完了）をクリックします。

最初のログオン

開始する前に、管理者アカウントで Windows にログオンし、Credential Manager にログオンしていないことが必要です。

1. 通知領域内の[HP ProtectTools Security Manager]（HP ProtectTools セキュリティ マネージャ）アイコンをダブルクリックして、HP ProtectTools セキュリティ マネージャを起動します。[HP ProtectTools Security Manager]ウィンドウが開きます。
2. 左側のパネルで**[Credential Manager]**（証明書マネージャ）をクリックしてから、右側のパネルの右上隅にある**[Log On]**（ログオン）をクリックします。[Credential Manager Logon Wizard]（証明書マネージャ ログオン ウィザード）が起動します。
3. **[Password]**（パスワード）ボックスに Windows パスワードを入力して**[Next]**をクリックします。

証明書の登録

[My Identity]（個人 ID）ページを使用して、各種の認証方法、または証明書を登録できます。登録が完了した後、それらの方法を使用して Credential Manager にログオンできます。

指紋の登録

指紋認証システムでは、Windows パスワードではなく、指紋を使用して認証することで Windows にログオンできます。

指紋認証システムのセットアップ

1. Credential Manager にログオンしたら、指紋認証システムに指を押し当てます。[Credential Manager Registration Wizard]（証明書マネージャ登録ウィザード）が起動します。

2. **[Next]**（次へ）をクリックします。

   注記　初期設定では、2 種類以上の指紋を登録する必要があります。

   最初の指紋登録に使用する指は、初期設定では右の人差し指です。初期設定を変更するには、最初の登録に使用したい右手または左手の指をクリックします。クリックされた指は、選択されたことを表すために強調表示されます。

3. 指紋センサに指を押し当てて、ゆっくりと下方向に滑らせます。ウィザードの説明に沿って操作し、画面に表示される指が緑色に変わるまで、同じ指の押し当てを繰り返します。

   注記　指紋を登録するには、複数回の押し当てが必要です。

   指紋登録の作業を中断して初めからやり直す場合は、画面で強調表示されている指を右クリックして**[Clear]**（消去）または**[Clear All]**（すべて消去）をクリックします。

4. ウィザードの説明に沿って操作し、2 つ目の指紋を登録します。

   注記　2 種類以上の指紋を登録する前に**[Finish]**をクリックすると、エラー メッセージが表示されます。続行するには、**[OK]**をクリックします。

5. 2 種類以上の指紋を正しく登録できたら、**[Next]**（次へ）をクリックします。

6. 指紋認証により Windows にログオンしたい場合は、**[Yes, I want to use Credential Manager to logon to Windows]**（はい、Windows へのログオンに証明書マネージャを使用します）チェック ボックスにチェックを入れます。**[Finish]**（完了）をクリックします。

7. 別の Windows ユーザ用の指紋を登録するには、そのユーザとして Windows にログオンして手順 1 ～ 6 を繰り返します。

登録された指紋を使用した Windows へのログオン

1. 指紋を登録したらすぐに Windows を再起動します。

2. Windows の[ようこそ]画面で、登録された指のどれかを押し当てて Windows にログオンします。

Java Card、スマート カード、トークン、または仮想トークンの登録

注記　この手順を実行するには、スマート カード リーダーを設定しておく必要があります。リーダーが装備されていない場合は、「仮想トークンの作成」の説明に沿って仮想トークンを登録できます。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。

2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）をクリックします。

3. 右側のパネルで、**[Register Smart Card or Token]**（スマート カードまたはトークンの登録）をクリックします。[Credential Manager Registration Wizard]（証明書マネージャ登録ウィザード）が起動します。

4. **[Next]**（次へ）をクリックします。

5. 登録する認証方法をクリックして**[Next]**をクリックします。

6. 画面の説明に沿って操作し、登録を完了します。

USB eToken の登録

1. USB eToken ドライバがインストールされていることを確認します。

   注記　詳しくは、USB eToken の取扱説明書を参照してください。

2. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。

3. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）をクリックします。

4. 右側のパネルで、**[Register Smart Card or Token]**（スマート カードまたはトークンの登録）をクリックします。[Credential Manager Registration Wizard]（証明書マネージャ登録ウィザード）が起動します。

5. **[Next]**（次へ）をクリックします。

6. **[Device Type]**（デバイスの種類）で、**[USB eToken]→[Next]**（次へ）の順にクリックします。

7. 画面の説明に沿って操作し、登録を完了します。

その他の証明書の登録

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。

2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）をクリックします。

3. 右側のパネルで、**[Register Credentials]**（証明書の登録）をクリックします。[Credential Manager Registration Wizard]（証明書マネージャ登録ウィザード）が起動します。

4. **[Next]**（次へ）をクリックします。

5. 登録する認証方法をクリックして**[Next]**をクリックします。

6. 画面の説明に沿って操作し、登録を完了します。

一般的なタスク

Credential Manager の[My Identity]（個人 ID）ページには、すべてのユーザがアクセスできます。[My Identity]ページから、次のことができます。

- 仮想トークンの作成
- Windows ログオン パスワードの変更
- トークン PIN の管理
- ID の管理
- コンピュータのロック

注記　このオプションは、Credential Manager のクラシック ログオン プロンプトが有効に設定されている場合にのみ利用できます。「例 1：[Advanced Settings]（詳細設定）ページを使用して、Credential Manager からの Windows ログオンを可能にする方法」を参照してください。

仮想トークンの作成

仮想トークンの機能は、スマート カードや USB トークンとよく似ています。このトークンは、コンピュータのハードドライブ上か、Windows レジストリ内のどちらかに保存されます。仮想トークンでログオンすると、認証を完了するためにユーザ PIN の入力を要求されます。

新しい仮想トークンを作成するには、以下の手順で操作します。

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）をクリックします。
3. 右側のパネルで、**[Virtual Token]**（仮想トークン）をクリックします。[Credential Manager Registration Wizard]（証明書マネージャ登録ウィザード）が起動します。

   注記　[Virtual Token]オプションがない場合は、「その他の証明書の登録」の手順を実行します。
4. **[Next]**（次へ）をクリックします。
5. **[Virtual Token]**（仮想トークン）→**[Next]**の順にクリックします。
6. 仮想トークン ファイルの名前と場所を入力し（または、**[Browse]**（参照）をクリックしてファイルの場所を見つけ）、**[Next]**をクリックします。
7. マスタ PIN とユーザ PIN を設定して確定します。
8. **[Finish]**（完了）をクリックします。

Windows ログオン パスワードの変更

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）をクリックします。

3. 右側のパネルで、**[Change Windows Password]**（Windows パスワードの変更）をクリックします。

4. **[Old password]**（古いパスワード）ボックスに、古いパスワードを入力します。

5. **[New Password]**（新しいパスワード）ボックスおよび**[Confirm password]**（パスワードの確認）ボックスに新しいパスワードを入力します。

6. **[Finish]**（完了）をクリックします。

トークン PIN の変更

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。

2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）をクリックします。

3. 右側のパネルで、**[Change Token PIN]**（トークン PIN の変更）をクリックします。

4. PIN を変更するトークンを選択して**[Next]**をクリックします。

5. 画面の説明に沿って操作し、PIN の変更を完了します。

ID の管理

ID のバックアップ

データが損失したり、誤って削除されたりした場合に備えて、Credential Manager で ID をバックアップしておくことをおすすめします。

ID をバックアップするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。

2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）をクリックします。

3. 右側のパネルで、**[Backup Identity]**（ID のバックアップ）をクリックします。

4. バックアップする要素を選択して**[Next]**をクリックします。

5. [Device Type]（デバイスの種類）ページで、バックアップの格納に使用するデバイスの種類を選択して**[Next]**をクリックします。

   注記　バックアップ ファイルに選択したデバイスのパスワードまたは PIN が必要です。

6. 画面の説明に沿って操作し、**[Finish]**（完了）をクリックします。

ID の復元

ID を復元するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）をクリックします。
3. 右側のパネルで、**[Restore Identity]**（ID の復元）をクリックします。
4. [Device Type]（デバイスの種類）ページで、バックアップが格納されているデバイスの種類を選択して**[Next]**をクリックします。

   注記　バックアップ ファイルに選択したデバイスのパスワードまたは PIN が必要です。

5. 画面の説明に沿って操作し、**[Finish]**（完了）をクリックします。
6. 確認ダイアログ ボックスで**[Yes]**（はい）をクリックします。

システムからの ID の消去

注記　この操作は、Windows ユーザ アカウントに影響しません。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）をクリックします。
3. 右側のパネルで、**[Clear Identity for this Account]**（このアカウントの ID の消去）をクリックします。
4. 確認ダイアログ ボックスで**[Yes]**（はい）をクリックします。ID がログオフされ、システムから削除されます。

コンピュータのロック

この機能は、Credential Manager を使用して Windows にログオンした場合に利用できます。席を離れている間にコンピュータをセキュリティで保護するには、作業環境のロック機能を使用します。これにより、不正なユーザにコンピュータへのアクセスを入手される事態を防ぐことができます。このロックは、自分自身と、コンピュータ上の管理者グループのメンバのみが解除できます。

注記　このオプションは、Credential Manager のクラシック ログオン プロンプトが有効に設定されている場合にのみ利用できます。「例 1：[Advanced Settings]（詳細設定）ページを使用して、Credential Manager からの Windows ログオンを可能にする方法」を参照してください。

コンピュータのロック解除にスマート カード、指紋認証システム、またはトークンが必要となるように作業環境のロック機能を設定することで、セキュリティを強化できます。詳しくは、この章の「Credential Manager の設定」を参照してください。

コンピュータをロックするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）をクリックします。
3. 右側のパネルで、**[Lock Workstation]**（作業環境をロック）をクリックします。Windows のログオン画面が表示されます。コンピュータのロックを解除するには、Windows パスワードまたは[Credential Manager Logon Wizard]（証明書マネージャ ログオン ウィザード）を使用する必要があります。

Windows のログオンの使用

ローカル コンピュータまたはネットワーク ドメインのどちらでも、Credential Manager を使用して Windows にログオンできます。初めて Credential Manager にログオンすると、ローカルの Windows ユーザ アカウントが、Windows ログオン サービス用のアカウントとして自動的に追加されます。

Credential Manager を使用した Windows へのログオン

Credential Manager を使用して、Windows のネットワークまたはローカル アカウントにログオンできます。

1. Windows へのログオン用に指紋を登録してある場合は、指を押し当ててログオンします。
2. Windows へのログオン用に指紋を登録していない場合は、画面の左上隅にある指紋アイコンの隣のキーボード アイコンをクリックします。[Credential Manager Logon Wizard]（証明書マネージャ ログオン ウィザード）が起動します。
3. **[User name]**（ユーザ名）の矢印→自分の名前の順にクリックします。
4. **[Password]**（パスワード）ボックスにパスワードを入力して **Next**（次へ）をクリックします。

5. **[More]**（詳細）→**[Wizard Options]**（ウィザード オプション）の順に選択します。
   a. 次回コンピュータにログオンした時にこの名前を初期設定のユーザ名にする場合は、**[Use last user name on next logon]**（前回のユーザ名を次のログオン時に使用）チェック ボックスにチェックを入れます。
   b. このログオン ポリシーを初期設定の認証方法にする場合は、**[Use last policy on next logon]**（前回のポリシーを次のログオン時に使用）チェック ボックスにチェックを入れます。
6. 画面に表示される説明に沿って操作します。認証情報が正しい場合は、Windows アカウントおよび Credential Manager にログオンします。

アカウントの追加

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
3. 右側のパネルで、**[Windows Logon]**（Windows のログオン）→**[Add a Network Account]**（ネットワーク アカウントの追加）の順にクリックします。[Add Network Account Wizard]（ネットワーク アカウントの追加ウィザード）が起動します。
4. **[User name]**（ユーザ名）ボックスに新しいアカウントのユーザ名を入力するか、**[Browse]**（参照）をクリックしてユーザ名を見つけます。
5. 使用可能なドメインの一覧からドメインをクリックします。
6. パスワードを入力して確定します。

注記　Credential Manager でこのアカウントを認証したい場合は、**[Validate network account when Next or Finish button clicked]**（[次へ]または[完了]ボタンのクリック時にネットワーク アカウントを認証する）チェック ボックスにチェックが入っていることを確認します。

7. **[Finish]**（完了）をクリックします。

アカウントの削除

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
3. 右側のパネルで、**[Windows Logon]**（Windows のログオン）→**[Manage Network Accounts]**（ネットワーク アカウントの管理）の順にクリックします。**[Manage Network Accounts]**ダイアログ ボックスが表示されます。
4. 削除するアカウントをクリックして**[Remove]**（削除）をクリックします。
5. 確認ダイアログ ボックスで **[Yes]**（はい）をクリックします。
6. **[OK]**をクリックします。

シングルサインオンの使用

Credential Manager には、複数のインターネットおよび Windows プログラム用のユーザ名とパスワードを格納し、ユーザが登録されたプログラムにアクセスすると自動的にログオン証明書を入力する、シングルサインオン機能があります。

注記 シングルサインオンの重要な機能は、セキュリティとプライバシです。証明書はすべて暗号化されており、Credential Manager へのログオンに成功した後にだけ使用できます。

注記 セキュリティ保護されたサイトまたはプログラムにログオンする前に、スマート カード、指紋認証システム、またはトークンを使用して認証証明書を検証するように、シングルサインオンを設定することもできます。この機能は、銀行口座番号などの個人情報が含まれているプログラムまたは Web サイトにログオンする場合に特に有効です。詳しくは、この章の「Credential Manager の設定」を参照してください。

新しいアプリケーションの登録

Credential Manager では、Credential Manager にログオンしている間に起動するアプリケーションをすべて登録するよう要求されます。アプリケーションを手動で登録することもできます。

自動登録の使用

1. ログオンが必要なアプリケーションを起動します。
2. プログラムまたは Web サイトのパスワード ダイアログ ボックスで[Credential Manager SSO]（証明書マネージャ シングルサインオン）アイコンをクリックします。
3. プログラムまたは Web サイトのパスワードを入力して**[OK]**をクリックします。[Credential Manager Single Sign On]（証明書マネージャ シングルサインオン）ダイアログ ボックスが開きます。
4. **[More]**（詳細）をクリックして以下のオプションのどれかを選択します。
    - [Do not use SSO for this site or application.]（このサイトまたはアプリケーションではシングルサインオン（SSO）を使用しない。）
    - [Prompt to select account for this application.]（このアプリケーションのアカウントの選択画面を表示する。）
    - [Fill in credentials but do not submit.]（証明書に入力するが送信はしない。）
    - [Authenticate user before submitting credentials.]（証明書を送信する前にユーザ認証を行う。）
    - [Show SSO shortcut for this application.]（このアプリケーションの SSO ショートカットを表示する。）
5. **[Yes]**（はい）をクリックして、登録を完了します。

手動（ドラッグ アンド ドロップ）登録の使用

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。

3. 右側のパネルで、**[Single Sign On]**（シングルサインオン）→**[Register New Application]**（新しいアプリケーションの追加）の順にクリックします。[SSO Application Wizard]（SSO アプリケーション ウィザード）が起動します。
4. 登録するアプリケーションを、パスワード ボックスを含むページが表示されるまで操作します。
5. [SSO Application Wizard]（SSO アプリケーション ウィザード）の[Drag and Drop Registration]（ドラッグ アンド ドロップ登録）ページで、自動化する操作の種類を選択します。

> **注記** ほとんどの場合、自動化する操作は**[Logon simple dialog]**（ログオン簡易ダイアログ）です。

6. ウィザード ページのアイコンをクリックし、パスワード ボックスが表示されているアプリケーションの領域までドラッグします。その領域が強調表示されたら、ポインタでの選択を解除します。
7. [SSO Application Wizard]（SSO アプリケーション ウィザード）の[Application Information]（アプリケーション情報）ページで、アプリケーションの名前と説明を入力します。
8. **[Finish]**（完了）をクリックします。
9. ログオン証明情報（たとえば、ユーザ名とパスワード）をアプリケーション ボックスに入力します。
10. [Credential Manager Single Sign On]（証明書マネージャ シングルサインオン）ダイアログ ボックスで、証明書の名前を確定するか、名前を右クリックして変更します。 **[Yes]**（はい）をクリックします。
11. **[More]**（詳細）をクリックして以下のオプションのどれかを選択します。
    - [Do not use SSO for this site or application.]（このサイトまたはアプリケーションではシングルサインオン（SSO）を使用しない。）
    - [Prompt to select account for this application.]（このアプリケーションのアカウントの選択画面を表示する。）
    - [Fill in credentials but do not submit.]（証明書に入力するが送信はしない。）
    - [Authenticate user before submitting credentials.]（証明書を送信する前にユーザ認証を行う。）
    - [Show SSO shortcut for this application.]（このアプリケーションの SSO ショートカットを表示する。）
12. **[Yes]**（はい）をクリックして、登録を完了します。

アプリケーションと証明書の管理

アプリケーション プロパティの変更

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
3. 右側のパネルの**[Single Sign On]**（シングルサインオン）で、**[Manage Applications and Credentials]**（アプリケーションおよび証明書の管理）をクリックします。

4. 変更するアプリケーション エントリをクリックして**[Properties]**.（プロパティ）をクリックします。

5. **[General]**（全般）タブをクリックして、アプリケーション名および説明を変更します。該当する設定の横にあるチェック ボックスにチェックを入れるか外して、設定を変更します。

6. **[Script]**（スクリプト）タブをクリックして、SSO アプリケーション スクリプトを表示し、編集します。

7. **[OK]**をクリックして変更を保存します。

シングルサインオンからのアプリケーションの削除

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。

2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。

3. 右側のパネルの**[Single Sign On]**（シングルサインオン）で、**[Manage Applications and Credentials]**（アプリケーションおよび証明書の管理）をクリックします。

4. 削除するアプリケーション エントリをクリックして**[Remove]**（削除）をクリックします。

5. 確認ダイアログ ボックスで**[Yes]**（はい）をクリックします。

6. **[OK]**をクリックします。

アプリケーションのエクスポート

アプリケーションをエクスポートして、シングルサインオン アプリケーション スクリプトのバックアップ コピーを作成できます。このファイルは、後でシングルサインオン データの復元に使用できます。これは、証明情報だけが含まれている ID バックアップ ファイルを補うものとして機能します。

アプリケーションをエクスポートするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。

2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。

3. 右側のパネルの**[Single Sign On]**（シングルサインオン）で、**[Manage Applications and Credentials]**（アプリケーションおよび証明書の管理）をクリックします。

4. エクスポートするアプリケーション エントリをクリックします。**[More]**（詳細）→**[Applications]**（アプリケーション）→**[Export Script]**（スクリプトのエクスポート）の順にクリックします。

5. 画面の説明に沿って操作し、エクスポートを完了します。

6. **[OK]**をクリックします。

アプリケーションのインポート

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。

2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。

3. 右側のパネルの**[Single Sign On]**（シングルサインオン）で、**[Manage Applications and Credentials]**（アプリケーションおよび証明書の管理）をクリックします。

4. インポートするアプリケーション エントリをクリックします。**[More]**（詳細）→**[Applications]**（アプリケーション）→**[Import Script]**（スクリプトのインポート）の順に選択します。

5. 画面の説明に沿って操作し、インポートを完了します。

6. **[OK]**をクリックします。

証明書の変更

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。

2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。

3. 右側のパネルの**[Single Sign On]**（シングルサインオン）で、**[Manage Applications and Credentials]**（アプリケーションおよび証明書の管理）をクリックします。

4. 変更するアプリケーション エントリをクリックして**[More]**（詳細）をクリックします。

5. 以下のオプションのどれかを選択します。

   - Applications（アプリケーション）
     - Add New（新しく追加）
     - Remove（削除）
     - Properties（プロパティ）
     - Import Script（スクリプトのインポート）
     - Export Script（スクリプトのエクスポート）
   - 証明書
     - Create New（新しく作成）
   - View Password（パスワードの表示）

   注記　パスワードを表示するには、事前に ID の認証を行う必要があります。

6. 画面に表示される説明に沿って操作します。

7. **[OK]**をクリックして変更を保存します。

[Application Protection]（アプリケーションの保護）の使用

この機能を使用して、アプリケーションへのアクセス設定を行えます。以下の基準に基づいてアクセスを制限できます。

- ユーザのカテゴリ
- 使用する時間
- 無操作の状態

アプリケーションへのアクセス制限

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
3. 右側のパネルの**[Application Protection]**（アプリケーションの保護）で、**[Manage Protected Applications]**（保護されたアプリケーションの管理）をクリックします。[Application Protection Service]（アプリケーション保護サービス）ダイアログ ボックスが表示されます。
4. アクセスを管理したいユーザのカテゴリを選択します。

注記　カテゴリが[Everyone]（全員）でない場合は、[Everyone]カテゴリ以外を優先させるために**[Override default settings]**（初期設定以外を優先する）を選択する必要がある場合があります。

5. **[追加]**をクリックします。[Add a Program Wizard]（プログラムの追加ウィザード）が起動します。
6. 保護するアプリケーションをクリックして**[OK]**をクリックします。そのアプリケーションの[Properties]（プロパティ）ダイアログ ボックスが開きます。
7. **[General]**（全般）タブをクリックします。以下の設定のどれかを選択します。
   - [Disabled (Cannot be used)]（無効（使用不可））
   - [Enabled (Can be used without restrictions)]（有効（無制限に使用可能））
   - [Restricted (Usage depends on settings)]（制限あり（使用制限は設定により異なる））
8. 使用制限ありの設定を選択した場合、以下の設定が利用可能になります。
   a. 時間、曜日、または日付に基づいて使用を制限する場合は、**[Schedule]**（スケジュール）タブをクリックして設定を行います。
   b. 無操作状態に基づいて使用を制限する場合は、**[Advanced]**（詳細）タブをクリックして無操作の期間を選択します。
9. **[OK]**をクリックして、アプリケーションの[Properties]（プロパティ）ダイアログ ボックスを閉じます。
10. **[OK]**をクリックします。

アプリケーションの保護の解除

アプリケーションのアクセス制限を解除するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
3. 右側のパネルの**[Application Protection]**（アプリケーションの保護）で、**[Manage Protected Applications]**（保護されたアプリケーションの管理）をクリックします。[Application Protection Service]（アプリケーション保護サービス）ダイアログ ボックスが表示されます。

4. アクセスを管理したいユーザのカテゴリを選択します。

注記　カテゴリが[Everyone]（全員）でない場合は、[Everyone]カテゴリ以外を優先させるために**[Override default settings]**（初期設定以外を優先する）をクリックする必要がある場合があります。

5. 削除するアプリケーション エントリをクリックして**[Remove]**（削除）をクリックします。
6. **[OK]**をクリックします。

保護されたアプリケーションの制限設定の変更

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
3. 右側のパネルの**[Application Protection]**（アプリケーションの保護）で、**[Manage Protected Applications]**（保護されたアプリケーションの管理）をクリックします。[Application Protection Service]（アプリケーション保護サービス）ダイアログ ボックスが表示されます。
4. アクセスを管理したいユーザのカテゴリを選択します。

注記　カテゴリが[Everyone]（全員）でない場合は、[Everyone]カテゴリ以外を優先させるために**[Override default settings]**（初期設定以外を優先する）をクリックする必要がある場合があります。

5. 変更するアプリケーションをクリックして**[Properties]**（プロパティ）をクリックします。そのアプリケーションの[Properties]（プロパティ）ダイアログ ボックスが開きます。
6. **[General]**（全般）タブをクリックします。以下の設定のどれかを選択します。
   - [Disabled (Cannot be used)]（無効（使用不可））
   - [Enabled (Can be used without restrictions)]（有効（無制限に使用可能））
   - [Restricted (Usage depends on settings)]（制限あり（使用制限は設定により異なる））
7. [Restricted]（制限あり）を選択した場合、以下の設定が利用可能になります。
   a. 時間、曜日、または日付に基づいて使用を制限する場合は、**[Schedule]**（スケジュール）タブをクリックして設定を行います。
   b. 無操作状態に基づいて使用を制限する場合は、**[Advanced]**（詳細）タブをクリックして無操作の期間を選択します。
8. **[OK]**をクリックして、アプリケーションの[Properties]（プロパティ）ダイアログ ボックスを閉じます。
9. **[OK]**をクリックします。

高度なタスク（管理者のみ）

Credential Manager の[Authentication and Credentials]（認証および証明書）ページおよび[Advanced Settings]（詳細設定）ページは、管理者権限を持つユーザだけが使用できます。これらのページから、次のタスクを実行できます。

- ユーザおよび管理者のログオン方法の指定
- カスタム認証要件の設定
- 証明書のプロパティの設定
- Credential Manager の設定

ユーザおよび管理者のログオン方法の指定

[Authentication and Credentials]（認証および証明書）ページで、ユーザまたは管理者のどちらかに、どのような証明書の種類または組み合わせが必要かを指定できます。

ユーザまたは管理者のログオン方法を指定するには、以下の手順で操作します。

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）→**[Authentication and Credentials]**（認証および証明書）の順にクリックします。
3. 右側のパネルで、**[Authentication]**（認証）タブをクリックします。
4. カテゴリの一覧から、カテゴリ（**[Users]**（ユーザ）または**[Administrators]**（管理者））をクリックします。
5. 一覧から、認証方法の種類または組み合わせをクリックします。
6. **[Apply]**（適用）→**[OK]**の順にクリックして変更を保存します。

カスタム認証要件の設定

[Authentication and Credentials]（認証および証明書）ページの[Authentication]（認証）タブに、必要な認証証明書のセットが一覧表示されない場合は、カスタム要件を作成できます。

カスタム要件を設定するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）→**[Authentication and Credentials]**（認証および証明書）の順にクリックします。
3. 右側のパネルで、**[Authentication]**（認証）タブをクリックします。
4. カテゴリの一覧から、カテゴリ（**[Users]**（ユーザ）または**[Administrators]**（管理者））をクリックします。
5. 認証方法の一覧から、**[Custom]**（カスタム）をクリックします。
6. **[Configure]**（設定）をクリックします。
7. 使用する認証方法を選択します。
8. 以下のどちらかをクリックして、方法の組み合わせを選択します。
   - AND を使用して認証方法を組み合わせる

     （ユーザはログオンするたびに、チェックを入れたすべての方法で認証する必要があります）
   - OR を使用して複数の認証方法のうち 1 つを要求する

     （ユーザはログオンするたびに、チェックを入れた方法のどれかを選択できます）
9. **[OK]**をクリックします。
10. **[Apply]**（適用）→**[OK]**の順にクリックして変更を保存します。

証明書のプロパティの設定

[Authentication and Credentials]（認証および証明書）ページの[Credentials]（証明書）タブで、使用可能な認証方法の一覧を表示して設定を変更できます。

証明書を設定するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）→**[Authentication and Credentials]**（認証および証明書）の順にクリックします。
3. 右側のパネルで、**[Credentials]**（証明書）タブをクリックします。

4. 変更する証明書の種類をクリックします。
   - 証明書を登録するには、**[Register]**（登録）をクリックし、画面の説明に沿って操作します。
   - 証明書を削除するには、**[Clear]**（クリア）をクリックし、確認ダイアログ ボックスで**[Yes]**（はい）をクリックします。
   - 証明書のプロパティを変更するには、**[Properties]**（プロパティ）をクリックし、画面の説明に沿って操作します。
5. **[適用]**→**[OK]**の順にクリックします。

Credential Manager の設定

[Settings]（設定）ページから、以下のタブを使用して各種の設定にアクセスし、変更することができます。

- General（全般）：基本的な設定を変更できます。
- Single Sign On（シングルサインオン）：現在のユーザに対するシングルサインオンの動作方法の設定（たとえば、ログオン画面の検出、登録されたログオン ダイアログへの自動ログオン、パスワードの表示などの処理方法）を変更できます。
- Services and Applications（サービスおよびアプリケーション）：使用可能なサービスを表示して、それらのサービスの設定を変更できます。
- Security（セキュリティ）：指紋認証ソフトウェアを選択して、指紋認証システムのセキュリティ レベルを調整できます。
- Smart Cards and Tokens（スマート カードおよびトークン）：使用可能なすべてのスマート カードおよびトークンのプロパティを表示して変更できます。

Credential Manager の設定を変更するには、以下の手順で操作します。

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）→**[Settings]**（設定）の順にクリックします。
3. 右側のパネルで、変更する設定が含まれるタブをクリックします。
4. 画面の説明に沿って操作し、設定を変更します。
5. **[Apply]**（適用）→**[OK]**の順にクリックして変更を保存します。

例 1：[Advanced Settings]（詳細設定）ページを使用して、Credential Manager からの Windows ログオンを可能にする方法

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）→**[Settings]**（設定）の順にクリックします。
3. 右側のパネルで、**[General]**（全般）タブをクリックします。

4. **[Select the way users log on to Windows (requires restart)]**（ユーザが Windows へログオンする方法の選択（再起動が必要））で、**[Use Credential Manager with classic logon prompt]**（証明書マネージャでクラシック ログオン プロンプトを使用する）チェック ボックスにチェックを入れます。

5. **[Apply]**（適用）→**[OK]**の順にクリックして変更を保存します。

6. コンピュータを再起動します。

注記　**[Use Credential Manager with classic logon prompt]**（証明書マネージャでクラシック ログオン プロンプトを使用する）チェック ボックスにチェックを入れると、コンピュータをロックできるようになります。「コンピュータのロック」を参照してください。

例 2：[Advanced Settings]（詳細設定）ページを使用して、シングルサインオンの前にユーザ確認を要求する方法

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明書マネージャ）→**[Settings]**（設定）の順にクリックします。
3. 右側のパネルで、**[Single Sign On]**（シングルサインオン）タブをクリックします。
4. **[When registered logon dialog or Web page is visited]**（登録したログオン ダイアログまたは Web ページが表示された時の動作）で、**[Authenticate user before submitting credentials]**（証明書を送信する前にユーザの認証を行う）チェック ボックスにチェックを入れます。
5. **[Apply]**（適用）→**[OK]**の順にクリックして変更を保存します。
6. コンピュータを再起動します。

7 Device Access Manager for HP ProtectTools

このセキュリティ ツールは、管理者だけが使用できます。Device Access Manager for HP ProtectTools では、コンピュータ システムに取り付けられたデバイスへの不正なアクセスに対するセキュリティ機能を提供します。これらのセキュリティ機能には、以下のものが含まれます。

- ユーザごとに作成されるデバイス プロファイルによる、デバイス アクセスの定義
- グループ メンバーシップ基づいた、デバイス アクセスの許可または拒否

バックグラウンド サービスの開始

デバイス プロファイルを適用するには、HP ProtectTools Device Locking/Auditing（HP ProtectTools デバイス ロック/検査）バックグラウンド サービスが実行されている必要があります。初めてデバイス プロファイルの適用を試みると、HP ProtectTools セキュリティ マネージャにより、バックグラウンド サービスを開始するかどうかを尋ねるダイアログ ボックスが表示されます。バックグラウンド サービスを開始し、またシステムが起動するたびに自動的に起動するように設定するには、**[はい]**をクリックします。

簡易構成

この機能を使用して、次のクラスのデバイスへのアクセスを拒否できます。

- 管理者以外のすべての USB デバイス
- 管理者以外のすべてのリムーバブル メディア（フロッピーディスク、USB メモリなど）
- 管理者以外のすべての DVD/CD-ROM ドライブ
- 管理者以外のすべてのシリアル ポートおよびパラレル ポート

管理者以外のすべてのユーザによるデバイス クラスへのアクセスを拒否するには、以下の手順で操作します。

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Device Access Manager]**（デバイス アクセス マネージャ）→**[簡易構成]**の順にクリックします。
3. 右側のパネルで、アクセスを拒否するデバイスのチェック ボックスにチェックを入れます。
4. **[適用]**をクリックします。

注記　バックグラウンド サービスが実行されていない場合は、ここで起動が試みられます。**[はい]**をクリックして許可します。

5. **[OK]**をクリックします。

デバイス クラス構成（詳細設定）

特定のユーザ、またはユーザ グループによる、特定のデバイスの種類へのアクセスを許可または拒否するための選択項目も利用できます。

ユーザまたはグループの追加

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Device Access Manager]**（デバイス アクセス マネージャ）→**[デバイス クラス構成]**の順にクリックします。
3. デバイスのリストで、設定するデバイス クラスをクリックします。
4. **[追加]**をクリックします。[Select Users or Groups]（ユーザまたはグループの選択）ダイアログ ボックスが表示されます。
5. **[Advanced]**（詳細）→**[Find Now]**（今すぐ検索）の順に選択して、追加するユーザまたはグループを検索します。
6. アクセスを拒否するユーザをクリックして**[OK]**をクリックします。
7. **[OK]**をクリックします。

ユーザまたはグループの削除

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Device Access Manager]**（デバイス アクセス マネージャ）→**[デバイス クラス構成]**の順にクリックします。
3. デバイスのリストで、設定するデバイス クラスをクリックします。
4. 削除するユーザまたはグループをクリックして**[削除]**をクリックします。
5. **[適用]**→**[OK]**の順にクリックします。

ユーザまたはグループのアクセス拒否

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Device Access Manager]**（デバイス アクセス マネージャ）→**[デバイス クラス構成]**の順にクリックします。
3. デバイスのリストで、設定するデバイス クラスをクリックします。
4. **[ユーザ/グループ]**で、アクセスを拒否するユーザまたはグループを追加します。
5. アクセスを拒否するユーザまたはグループの隣の**[拒否]**をクリックします。
6. **[適用]**→**[OK]**の順にクリックします。

グループの単一ユーザによるデバイス クラスへのアクセス許可

単一のユーザによるデバイス クラスへのアクセスを許可し、そのユーザのグループのその他のメンバーによるアクセスは拒否するように設定できます。

単一のユーザによるアクセスは許可し、グループには許可しないように設定するには、以下の手順で操作します。

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Device Access Manager]**（デバイス アクセス マネージャ）→**[デバイス クラス構成]**の順にクリックします。
3. デバイスのリストで、設定するデバイス クラスをクリックします。
4. **[ユーザ/グループ]**で、アクセスを拒否するグループを追加します。
5. アクセスを拒否するグループの隣の**[拒否]**をクリックします。
6. 目的のクラスの下のフォルダに移動し、特定のユーザを追加します。**[Allow]**（許可）をクリックして、そのユーザによるアクセスを許可します。
7. **[適用]**→**[OK]**の順にクリックします。

グループの単一ユーザによる特定のデバイスへのアクセス許可

単一のユーザによる特定のデバイスへのアクセスを許可し、そのユーザのグループのその他のメンバーによる、クラス内のすべてのデバイスへのアクセスは拒否するように設定できます。

特定のデバイスへのアクセスを単一のユーザには許可し、グループには許可しないように設定するには、以下の手順で操作します。

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Device Access Manager]**（デバイス アクセス マネージャ）→**[デバイス クラス構成]**の順にクリックします。
3. デバイスのリストで、設定するデバイス クラスをクリックして、その下のフォルダに移動します。
4. **[ユーザ/グループ]**で、アクセスを拒否するグループを追加します。
5. アクセスを拒否するグループの隣の**[拒否]**をクリックします。
6. デバイス リストで、ユーザによるアクセスを許可する特定のデバイスに移動します。
7. **[追加]**をクリックします。[Select Users or Groups]（ユーザまたはグループの選択）ダイアログ ボックスが表示されます。
8. **[Advanced]**（詳細）→**[Find Now]**（今すぐ検索）の順に選択して、追加するユーザまたはグループを検索します。
9. アクセスを許可するユーザをクリックして**[OK]**をクリックします。
10. **[Allow]**（許可）をクリックして、そのユーザによるアクセスを許可します。
11. **[適用]**→**[OK]**の順にクリックします。

用語集

BIOS セキュリティ モード　有効にすると、ユーザ認証にスマート カードおよび有効な PIN の使用が必要になる、スマート カード セキュリティでの設定。

BIOS プロファイル　他のアカウントに保存および適用できる、BIOS 設定値の集合。

DriveLock　ハードドライブをユーザにリンクして、コンピュータの起動時にユーザに正しい DriveLock パスワードの入力を要求するセキュリティ機能。

ID　HP ProtectTools Credential Manager 内で、特定のユーザのアカウントまたはプロファイルのように処理される、証明書と設定の集合。

Java Card　所有者に関する識別情報が格納されている、サイズと形状がクレジット カードに似た小さなハードウェア。所有者をコンピュータに対して認証するために使用されます。

PSD（Personal Secure Drive）　機密情報を保護するための記憶領域を提供する機能。

TPM（Trusted Platform Module）内蔵セキュリティ チップ（一部のモデルのみ）　機密性の高いユーザ情報を悪意のある攻撃者から保護できる、統合されたセキュリティ チップ。特定のプラットフォーム上の信頼性の基盤です。TPM によって、TCG（Trusted Computing Group）仕様に適合する暗号化アルゴリズムおよび演算方法が提供されます。

USB トークン　ユーザに関する識別情報が格納されているセキュリティ デバイス。スマート カードや指紋認証システムと同様に、所有者をコンピュータに対して認証するために使用されます。

Windows ユーザ アカウント　ネットワークまたは個別のコンピュータへのログオンを承認された個人のプロファイル。

シングルサインオン　認証情報を格納し、パスワード認証が必要なインターネットおよび Windows アプリケーションに Credential Manager を使用してアクセスできるようにする機能。

スマート カード　所有者に関する識別情報が格納されている、サイズと形状がクレジット カードに似た小さなハードウェア。所有者をコンピュータに対して認証するために使用されます。

スマート カードのユーザ パスワード　起動時または再起動時の識別のために、[Computer Setup]でユーザ スマート カードをコンピュータにリンクするパスワード。このパスワードは、管理者が手動で設定することも、ランダムに生成することもできます。

スマート カードの管理者パスワード　起動時または再起動時の識別のために、[Computer Setup]で管理者スマート カードをコンピュータにリンクするパスワード。このパスワードは、管理者が手動で設定することも、ランダムに生成することもできます。

デジタル署名　資料の送信者を証明し、署名された後にファイルが変更されていないことを証明するファイルとともに送信されるデータ。

デジタル証明書　デジタル証明書の所有者の身元と、デジタル情報の署名に使用される電子キーのペアとを結びつけることによって、個人または企業の身元を証明する電子的な信用証明書。

ドメイン　ネットワークの一部であり、共通のディレクトリ データベースを共有するコンピュータの集合。ドメインには一意の名前が付けられ、各ドメインには一連の共通の規則および手順が設定されます。

ネットワーク アカウント　ローカル コンピュータ上、ワークグループ内、またはドメイン上の Windows ユーザまたは管理者のアカウント。

バイオメトリック　指紋などの身体的な特徴を使用してユーザを識別する認証証明のカテゴリ。

リブート　コンピュータを再起動するプロセス。

暗号化　権限のない受信者がデータを解読できないように平文を暗号文に変換するための、暗号法で使用されるアルゴリズムなどの手順。データの暗号化にはさまざまな種類があり、ネットワーク セキュリティの基礎として使用されます。一般的な暗号化には、データ暗号化規格（DES）や公開キー暗号があります。

暗号化サービス プロバイダ（CSP）　明確なインタフェースを使用して特定の暗号化関数を実行するための暗号化アルゴリズムの提供者またはライブラリ。

暗号化の解除　暗号化されたデータを平文に変換するための、暗号法で使用される手順。

暗号化ファイル システム（EFS）　選択されたフォルダ内のすべてのファイルおよびサブフォルダを暗号化するシステム。

暗号法　特定の個人だけが解読できるように、データを暗号化および暗号化解除する手法。

移行　キーおよび証明書を管理、復元、および転送する作業。

仮想トークン　スマート カードやリーダーとよく似た働きをするセキュリティ機能。このトークンは、コンピュータのハードドライブ上か、Windows レジストリ内のどちらかに保存されます。仮想トークンでログオンすると、認証を完了するためにユーザ PIN の入力を要求されます。

緊急リカバリ アーカイブ　他のプラットフォームの所有者キーを使用して基本ユーザ キーを再暗号化できる、保護された記憶領域。

厳重なセキュリティ　電源投入時パスワード、管理者パスワード、およびその他の形態の、電源投入時認証に対する保護機能を強化する、BIOS Configuration にあるセキュリティ機能。

公開キー基盤（PKI）　証明書および暗号化キーを作成、使用、および管理するためのインタフェースを定義する規格。

自動 DriveLock　DriveLock パスワードが生成され、TPM 内蔵セキュリティ チップによって保護されるようにするセキュリティ機能。起動時にユーザが正しい TPM 基本ユーザ キーのパスワードを入力し、それが TPM 内蔵セキュリティ チップによって認証されると、BIOS によってそのユーザ用のハードドライブのロックが解除されます。

証明書　ユーザが認証プロセスで特定のタスクに対する適格性を証明するための方法。

電源投入時認証　スマート カード、セキュリティ チップ、パスワードなど、コンピュータの起動時に何らかの形式の認証を要求するセキュリティ機能。

認証　ユーザがタスクの実行（たとえば、コンピュータへのアクセス、特定のプログラムの設定変更、セキュリティ保護されたデータの表示など）を承認されているかどうかを確認するプロセス。

認証機関　公開キー基盤の運営に必要な証明書を発行するサービス。

索引

す

せ

て

と

ね

は

ふ

む

ゆ